INTERNATIONAL LAW STUDIES

UNITED STATES NAVAL WAR COLLEGE

INTERNATIONAL LAW DEPARTMENT

VOLUME 89

2013

International Law Studies

Volume 89

Naval War College
Newport, Rhode Island
2013

EDITORIAL OFFICE
International Law Studies
International Law Department
Naval War College (36)
686 Cushing Road
Newport, RI 02841-1207
Telephone: +1-401-841-4949
DSN: 841-4949
E-mail: ILD@usnwc.edu

Website: http://www.usnwc.edu/ild

The International Law Studies ("Blue Book") series was initiated by the Naval War College in 1895 to publish essays, treatises and articles that contribute to the broader understanding of international law .

International Law Studies

Volume 89

Board of Advisors

Stockton Chair of International Law

2013 –	Michael N. Schmitt
2012- 2013	Wolff Heintschel von Heinegg
2010-2012	Ken Watkin
2009-2010	Derek Jinks
2008-2009	Richard J. Grunawalt
2007-2008	Michael N. Schmitt
2006-2007	Craig H. Allen
2005-2006	Jane Dalton
2004-2005	Charles Garraway
2003-2004	Wolff Heintschel von Heinegg
2002-2003	Yoram Dinstein
2001-2001	Nicholas Rostow
2000-2001	Ivan Shearer
1999-2000	Yoram Dinstein
1998-1999	Ruth Wedgwood
1996-1998	Leslie C. Green
1995-1996	Myron H. Nordquist
1994-1995	Robert F. Turner
1993-1994	Richard J. Grunawalt
1992-1993	George K. Walker
1991-1992	Horace B. Robertson, Jr.
1990-1991	John H. McNeill
1989-1990	Alberto R. Coll
1986-1989	Richard J. Grunawalt
1985-1986	George Bunn
1984-1985	W. Hays Parks
1983-1984	George Bunn
1982-1983	Jon L. Jacobson
1981-1982	Alfred P. Rubin
1980-1981	John F. Murphy
1979-1980	Hamilton DeSaussure
1977-1979	Gordon Christenson
1975-1977	Vacant
1974-1975	William T. Mallison, Jr.
1972-1974	Alwyn V. Freeman
1971-1972	Howard S. Levie
1970-1971	L. F. E. Goldie
1969-1970	Oliver J. Lissitzyn
1968-1969	Richard B. Lillich
1967-1968	John H. Spencer
1966-1967	Dennis M. O'Connor
1965-1966	James F. Hogg
1964-1965	Vacant
1963-1964	Gordon B. Baldwin
1962-1963	Carl Q. Christol
1961-1962	Neill H. Alford, Jr.
1960-1961	William T. Mallison, Jr.
1959-1960	Carl M. Franklin
1958-1959	Roland J. Stanger
1957-1958	Vacant
1956-1957	Ralph G. Jones
1955-1956	Brunson MacChesney
1954-1955	Leo Gross
1953-1954	Hans Kelsen
1951-1953	Manley O. Hudson

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

The Geography of Cyber Conflict: Through a Glass Darkly

Ashley Deeks

89 INT'L L. STUD. 1 (2013)

Volume 89 2013

The Geography of Cyber Conflict: Through a Glass Darkly

Ashley Deeks[*]

I. INTRODUCTION

Imagine an Israeli Air Force jet is shot down in international airspace just outside Turkish airspace. Imagine further that the Israel Defense Forces (IDF) and Israeli intelligence services quickly ascertain with a high level of confidence that a Hezbollah cell located in Turkey was responsible for the shoot-down. Israel now confronts a difficult question: having suffered an armed attack, may it use force in self-defense against a non-state actor in the territory of a state with which it is not in an armed conflict and that was not the author of the attack?

In previous work, I have argued that Israel may only take action in Turkish territory against Hezbollah if it has Turkish consent or if it determines that Turkey is unwilling or unable to suppress the threat posed by Hezbollah.[1] This "unwilling or unable" test, which has analogical roots in

* Associate Professor of Law, University of Virginia School of Law.

1. *See generally* Ashley Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VIRGINIA JOURNAL OF INTERNATIONAL LAW 483 (2012).

the law of neutrality,[2] serves as an attempt to balance the security of the State that suffered the attack (the "victim State") against the sovereignty of the State from which the non-State actor launched the attack (the "territorial State"). The test also reflects the international community's interest in reducing to the lowest level feasible inter-State conflict (and State uses of force in self-defense).

Imagine now that the IDF learns that its air force's command and control center is being severely compromised electronically and has begun to send faulty coordinates to all of the IDF's military aircraft, including those currently airborne. As a result of the cyber attack,[3] the IDF loses communications with two of its jets, which crash into the Mediterranean Sea. Israel has a high level of confidence that several servers in Turkey are the source of the ongoing attack; additionally, the offending code behind the attack has Hezbollah's digital fingerprints on it and Israel has intelligence that Hezbollah has been trying for several years to conduct just such an attack. Assuming that Israel has the technological capacity to disable the Turkish servers currently routing the attack and believes that such an action is the only way to stop this attack, may Israel disable those Turkish servers (using cyber or kinetic tools)? What, if anything, must it do first?

This article argues that the "unwilling or unable" test applies to this scenario as well, although the issues facing Israel and Turkey in the two scenarios are different in important ways. Other scholars have suggested that the "unwilling or unable" test is relevant in the cyber context,[4] but no

---

2. J.M. SPAIGHT, WAR RIGHTS ON LAND 482 (1911) ("[W]here the neutral cannot or will not enforce its rights, then the belligerent is fully entitled to prevent the violation permitted by the neutral redounding to his disadvantage.").

3. This paper uses the phrase "cyber attacks" generically to refer to acts that "alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks," TECHNOLOGY, POLICY, LAW AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 1 (WILLIAM OWENS, KENNETH DAM, & HERBERT LIN, EDS., 2009) [hereinafter OWENS ET AL.]. A particular cyber attack may or may not constitute a use of force or armed attack, as those terms are used in the *jus ad bellum* sense.

4. *See* Duncan Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK LAW REVIEW 1023, 1050 (2007) ("International law contemplates that the [State injured by information operations] would notify the State from whose territory it believes the IO originated and request that State put a stop to it. The requested State is expected to comply with such requests . . . . Only if the requested State is unable or unwilling to stop the IO can the aggrieved State take counter-measures (or perhaps exercise a right of self-defense against the requested State . . . ."); George Walker, *Information Warfare and Neutrality*, 33 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 1079, 1199 (2000)

scholar has analyzed how a State actually should or would apply that test, how the test's application will differ in the cyber and non-cyber contexts and what that divergence teaches us about conflict in the cyber realm. This paper addresses those three issues, focusing on situations in which the cyber activity rises to the level of a cyber armed attack (rather than cyber activities that fall below that threshold). At the same time, it highlights the particular importance of State practice in adopting and expounding the use of the "unwilling or unable" test in the cyber context. Indeed, news reports suggest that the United States is wrestling mightily to determine when it is appropriate and lawful to take cyber action outside the boundaries of its own networks.[5] Establishing State-to-State expectations about what types of cyber activities will trigger what types of responses will provide important incentives for ostensibly neutral States to take steps to protect their computer networks while minimizing the likelihood of inter-State misunderstandings that lead to unnecessary conflict in the cyber or non-cyber realms.[6]

Part II describes the "unwilling or unable" test, including relevant factors that States should use in assessing whether another State has met that test. Part III applies those factors to the cyber context. Part IV considers how the U.S. government may be approaching these issues. Part V concludes.

II. THE "UNWILLING OR UNABLE" TEST

In the wake of the September 11 attacks, the United States concluded that it was in an international armed conflict with Al Qaeda, a non-State actor. Perhaps the most controversial aspect of this claim was the implicit argument that the United States therefore could use force against members of Al Qaeda anywhere they appeared. This concept resulted in the much-

("The 'means at a neutral's disposal' principle should be the test for a neutral's duty for belligerents' IW [information warfare] incursions; the neutral should be held to apply means at its disposal to detect and repel these incursions. Such being the case, the correlative right of a belligerent aggrieved by IW incursions should be that the belligerent may take such actions as are necessary in the territory of a neutral that is unable (or perhaps unwilling) to counter enemy IW force activities making unlawful use of that territory, a principle from the law of naval warfare.").

5. Ellen Nakashima, *Pentagon Proposes More Robust Role for Its Cyber-Specialists*, WASHINGTON POST, Aug. 9, 2012.

6. *See* OWENS ET AL., *supra* note 3, at 318 (explaining rationales behind legal regimes that regulate the development and use of certain kinds of weapons).

maligned idea of the "global war on terror." The United States later took care to clarify that its international armed conflict claim did not mean that it would use force in all countries in which members of Al Qaeda appeared. Rather, the United States asserted that it would only use force in those countries that either gave the United States consent to do so or were "unwilling or unable" to suppress the threat itself.[7] Nor is the United States the only State to employ the "unwilling or unable" test when evaluating the legality of using force against non-State actors in another State's territory. Israel, Russia and Turkey all have cited the test in recent years.[8] Scholars, too, have described the "unwilling or unable" test as the applicable test in this situation,[9] though some contest that the test has any status in international law.[10]

---

7. John B. Bellinger III, Legal Adviser, U.S. Department of State, Address at the London School of Economics: Legal Issues in the War on Terrorism (Oct. 31, 2006); Harold Koh, Legal Adviser, U.S. Department of State, Address at the Annual Meeting of American Society of International Law (Mar. 25, 2010).

8. *See* Deeks, *supra* note 1, at 486–87 (listing other States' claims).

9. *See, e.g.*, NOAM LUBELL, EXTRATERRITORIAL USE OF FORCE AGAINST NON-STATE ACTORS 42 (2010) (reciting the "unwilling or unable" test as the correct test for determining when a victim State may take measures against non-State actors in the territorial State); YORAM DINSTEIN, WAR, AGGRESSION, AND SELF-DEFENSE 217 (3d ed. 2001) ("Extraterritorial law enforcement is a form of self-defence, and it can be undertaken by Utopia against armed bands or terrorists inside Arcadian territory, in response to an armed attack unleashed by them from that territory. Utopia is entitled to enforce international law extraterritorially only when Arcadia is unable or unwilling to prevent repetition of that armed attack."); Carsten Stahn, *Terrorist Acts as "Armed Attack": The Right to Self-Defense, Article 51 (1/2) of the UN Charter, and International Terrorism*, 27 FLETCHER FORUM OF WORLD AFFAIRS JOURNAL 35, 47 (2003); Greg Travalio & John Altenburg, *Terrorism, State Responsibility, and the Use of Military Force*, 4 CHICAGO JOURNAL OF INTERNATIONAL LAW 97, 116 (2003) ("[S]hould a State be unwilling or unable to prevent its territory from being used as a sanctuary or base of operations by a transnational terrorist organization, a State threatened with an imminent attack by such an organization may . . . engage in a self-defense use of force to deal with this threat."); Alberto Coll, *The Legal and Moral Adequacy of Military Responses to Terrorism*, 81 AMERICAN SOCIETY INTERNATIONAL LAW PROCEEDINGS 297, 305 (1987) ("[O]nce it becomes reasonably evident that the harboring State is unable or unwilling to act, the injured State should be free to use the minimum of force required to stop the terrorist threat."); Ian Brownlie, *International Law and the Activities of Armed Bands*, 7 INTERNATIONAL & COMPARATIVE LAW QUARTERLY 712, 732 (1958) ("Military action across a frontier to suppress armed bands, which the territorial sovereign is unable or unwilling to suppress, has been explained in terms of legitimate self-defense on a limited number of occasions in the present century."); Tatiana Waisberg, *Colombia's Use of Force in Ecuador Against a Terrorist Organization*, 12 ASIL Insights (2008), *available at* http://www.asil.org/insights080822.cfm ("State practice and the UN Security Council's

Although this test plays a significant role in regulating the geography of an armed conflict (or the geographic location of a State's response to an armed attack), its precise substantive and procedural content remains unclear. Must the victim State request assistance from the territorial State before using force against the non-State actor in the territorial State? By what standards should the victim State evaluate the territorial State's proposed means to address the threat and its capacity to do so? In the context of an armed conflict, what level of threat justifies taking action, using the "unwilling or unable" theory? International law currently does not answer these questions.

As complicated as an "unwilling or unable" inquiry may be in the non-cyber context, it becomes even more complicated in the cyber context. First, it is far easier to employ the cyber infrastructure of third States for hostile ends than it is to employ the physical territory of those States to commit conventional hostile acts. States and non-State actors that are engaged in armed conflicts or that are intent on committing armed attacks tend to operate from a single State or from a limited number of States, by virtue of cost, politics, logistics and terrain. In contrast, those same States and non-State actors are able to employ the cyber infrastructure of a much larger number of third States in forcible pursuit of their goals. Second, the difficulty of attribution in the cyber context is well-known.[11] As a result, there will be many situations in which the victim State can ascertain that a third country's servers are being used for hostile purposes but be unable to identify with certainty the actual authors of the attacks. In some cases, the victim State may not even be able to identify the geographic origin of a given cyber attack.[12] This stands in contrast to kinetic activities outside the cyber context, where the victim State often is able to identify the authors of the armed attacks and their locations, using well-established intelligence and investigatory resources. Third, the increased anonymity of cyberspace

---

actions after the September 11 attacks may, however, indicate a trend toward recognizing that a State that suffers large-scale violence perpetrated by non-State actors located in another State has a right to use force in self-defense when . . . that other State proves unwilling or unable to reduce or eliminate the source of the violence.").

10. *See* Kevin Jon Heller, *The Unwilling or Unable Standard for Self-Defense*, OPINIO JURIS, (Sept. 17, 2011), http://opiniojuris.org/2011/09/17/the-unwilling-or-unable-standard-for-self-defense-against-non-State-actors/ (rejecting "unwilling or unable" test as customary international law on basis that there is insufficient State practice and evidence of *opinio juris*).

11. *See, e.g.*, Jack L. Goldsmith, *The New Vulnerability*, NEW REPUBLIC (June 7, 2010).

12. OWENS ET AL., *supra* note 3, at 294.

may mean growth in the number of actors that seek to use cyber attacks. The deterrence that accompanies the fear of getting caught is reduced because the chance of being held accountable is lower.

Before turning to the cyber scenarios in which a State will need to employ the "unwilling or unable" test, however, it is important to clarify several assumptions in this article. First, this piece assumes that cyber attacks that produce effects similar to those of kinetic military actions will constitute "armed attacks" that trigger the victim State's right of self-defense.[13] Second, it assumes that non-State actors may be authors of armed attacks, even when those attacks are not attributable to a State.[14] Third, it assumes that, in the context of an international armed conflict, it would not violate the law of neutrality for a neutral State to allow a belligerent State to use, or not prevent it from using, its public internet and communications networks as a conduit for a cyber attack.[15] It assumes, however, that neutrality law would prohibit a neutral State from allowing a State or non-State actor to use its tangible computer equipment or operating systems, including servers, to host those attacks.[16] This means that a victim State, in responding to

13. *See, e.g.*, Michael Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 929 (1998–99) (discussing possibility that computer network attacks could constitute "armed attacks"); Nils Melzer, *Cyberwarfare and International Law* 13, UNIDIR Resources (2011) (stating that cyber operations have the qualitative capacity to qualify as an armed attack within the meaning of UN Charter Article 51).

14. *See* Deeks, *supra* note 1, at 492–93 (describing three schools of thought on this question).

15. This follows from Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons during War on Land, art. 8. Oct 18, 1907, 36 Stat. 2310, 1 Bevans 654 [hereinafter Hague V], which States that a neutral power is not required to "forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."

16. *Id.* Allowing particular servers within the neutral State to host attacks is more closely akin to allowing a belligerent to move munitions of war across neutral territory or furnishing military supplies to a belligerent, which Hague V would prohibit. This seems to be the approach taken by the U.S. Department of Defense in 1999 in its Assessment of International Legal Issues in Information Operations. That document provides, "[U]se of a nation's communications networks as a conduit for an electronic attack would not be a violation of its sovereignty . . . . A transited State would have somewhat more right to complain if the attacking State obtained unauthorized entry into its computer systems as part of the communications path to the target computer. It would be even more offended if malicious logic directed against a target computer had some harmful effect against the transited State's own equipment, operating systems, or data." *See also* TALLINN MANUAL, Rule 92 (Michael Schmitt ed., forthcoming 2013); Eric Jensen, *Sovereignty and Neutrality in*

a cyber armed attack against it, would not violate Article 2(4) simply by directing its response through a third State's public communications channels. The victim State would trigger Article 2(4), however, if it damaged a server hosted in that third State.[17] Fourth, it assumes that the victim State will be able to direct its response in a manner consistent with both the *jus ad bellum* and the laws of armed conflict, including the principles of distinction and proportionality.[18] Finally, it assumes that, as a matter of policy, the victim State will conduct its responses to a cyber armed attack in the cyber realm, although there is no legal requirement that it do so.[19]

There are at least three scenarios in which a State that has suffered a cyber attack may seek to take responsive (forcible) action in a third State's territory and therefore will need to assess the third State's willingness and ability to take action to address that cyber attack. First, a State may be fighting another State in an international armed conflict, where the State's opponent has launched a cyber attack from a third State's territory. In international armed conflict, the laws of neutrality apply. Assuming that the third State is neutral in the international armed conflict, the laws of neutrality require the neutral State to prevent its territory from being used by a belligerent as a place from which to launch attacks.[20] If a belligerent nevertheless is initiating or conducting cyber attacks against another belligerent using the cyber infrastructure of a neutral State, the neutral State must

---

Cyber Conflict, 35 FORDHAM INTERNATIONAL LAW JOURNAL 815, 826–27 (2012) (arguing that the law of neutrality would require a neutral State to prevent a belligerent from initiating or facilitating an attack within neutral territory, but not to prevent the mere passage of malware or malicious code over its public cyber infrastructure); Melzer, *supra* note 13, at 20 (reasoning that neutral States can be expected to prevent belligerents from conducting "cyber hostilities" from within neutral territory but not the "routing of belligerent cyber operations through their publicly accessible communications infra-structure"); *but see* Davis Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 HARVARD INTERNATIONAL LAW JOURNAL 179, 210 (2006) (arguing that even allowing the transit of malicious code over a State's public internet infrastructure would violate that State's neutrality obligations).

17. Such an act would be akin to severing a telephone wire in a State, interrupting general telecommunications in that State.

18. Whether this requires the victim State to identify with certainty the nature and identity of the cyber attacker is not clear.

19. The U.S. cyber security strategy preserves the right to respond kinetically to a cyber armed attack. However, given the level of caution with which the U.S. government seems to be proceeding in crafting doctrine for cyber responses, it seems reasonable to assume that using kinetic force against a cyber armed attack, particularly in a third State's territory, would occur only in an extreme case.

20. Hague V, arts. 2, 4; TALLINN MANUAL, *supra* note 16, at Rule 93.

make efforts to terminate that use. If the neutral State is unwilling or unable to stop that belligerent, the belligerent's opponent may take forcible measures within the neutral State to do so.[21]

Second, a State may be in a non-international armed conflict, fighting against a non-State actor whose operations are primarily based either within that State or within a foreign State's territory. The non-State actor may undertake cyber actions during that conflict that utilize systems located in foreign States. In this case, one may reason by analogy to the law of neutrality to assert that the State fighting the non-international armed conflict may take measures in that foreign State to suppress the non-State actor's cyber attacks where the foreign State is unwilling or unable to do so itself.[22] The United States appears to believe that this is the appropriate test to apply in the context of kinetic armed conflicts against non-State actors that transcend a single State's borders.[23] It is not clear whether a victim State could respond forcibly to *any* cyber uses of force emanating from the third State, or if the victim State only could respond forcibly to those cyber uses of force that rise to the level of a cyber armed attack.[24]

---

21. *See* SPAIGHT, *supra* note 2, at 482; John Norton Moore, *Legal Dimensions of the Decision to Intercede in Cambodia*, 65 AMERICAN JOURNAL OF INTERNATIONAL LAW 38, 51 (1971) ("It is well established in customary international law that a belligerent Power may take action to end serious violations of neutral territory by an opposing belligerent when the neutral Power is unable to prevent belligerent use of its territory . . . ."); TALLINN MANUAL, *supra* note 16, at Rule 94.

22. Melzer, *supra* note 13, at 21 ("Strictly speaking, the law of neutrality applies only in international armed conflict. Arguably, however, the pragmatic logic of its core principles has already found its way into the practice of non-international armed conflicts as well."); International Committee of the Red Cross Official Statement of 8 March 2001 to the United Nations High Commissioner for Refugees Global Consultations on International Protection ("It is the ICRC's view that [Hague Convention V] can also be applied by analogy in situations of non-international armed conflicts, in which combatants either from the government side or from armed opposition groups have fled into a neutral State.").

23. Koh, *supra* note 7; John Brennan, Assistant to the President for Homeland Security and Counterterrorism, Address at Harvard Law School: Strengthening Our Security by Adhering to Our Values (Sept. 16, 2011), http://www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an.

24. The United States generally asserts that virtually all uses of force constitute armed attacks that trigger a State's right of self-defense. *See* William H. Taft IV, *Self-Defense and the* Oil Platforms *Decision*, 29 YALE JOURNAL OF INTERNATIONAL LAW 295, 299 (2004) (rejecting idea that attacks must rise to certain level of severity in order to qualify as armed attacks). Many States disagree with that position, however, and thus would have to confront how to respond to a use of cyber force short of an armed attack, launched by a non-

Third, a State that is not fighting an ongoing non-international armed conflict nevertheless may suffer a cyber armed attack from a non-State actor (or face an imminent threat thereof). This armed attack would trigger the victim State's right of self-defense under Article 51 of the U.N. Charter.[25] The victim State would then have to assess whether it was necessary to use force in self-defense against that non-State actor and, secondarily, whether it was necessary to use force *in that particular foreign State* against that non-State actor. If the territorial State is both willing and able to suppress the threat posed by that actor, it would not be necessary (and therefore would not be lawful) for the victim State to use force within the territorial's borders.

In each of these three scenarios, the victim State will be required to examine whether the territorial State can and will take action to halt or mitigate the attacks affecting the victim State. Although the test itself has traction in international law, its lack of substantive and procedural content makes it harder to apply and less legitimate as a restraining force in international relations. I previously suggested five principles, drawn from historical practice, that would help guide the test's application. These principles include the requirements that the victim State (1) prioritize cooperation or consent with the territorial State, rather than unilateral use of force; (2) ask the territorial State to address the threat and give it adequate time to respond; (3) reasonably assess the territorial State's capacity and control within the relevant region; (4) reasonably asses the territorial State's proposed

---

State actor extraterritorially. Those States might conclude that, absent an armed attack that triggers Article 51, the States cannot take any action in response that would violate Article 2(4) of the Charter. In practice, the United States actually may be imposing policy constraints on itself that bring it closer to that position. In his Harvard speech, John Brennan noted that "[b]ecause we are engaged in an armed conflict with al-Qa'ida, the United States takes the legal position that . . . we have the authority to take action against al-Qa'ida and its associated forces without doing a separate self-defense analysis each time." However, he also stated, "In practice, the U.S. approach to targeting in the conflict with al-Qa'ida is far more aligned with our allies' approach than many assume. This Administration's counterterrorism efforts outside of Afghanistan and Iraq are focused on those individuals who are a threat to the United States, whose removal would cause a significant – even if only temporary – disruption of the plans and capabilities of al-Qa'ida and its associated forces. Practically speaking, then, the question turns principally on how you define 'imminence.'" Brennan, *supra* note 23.

25. In the context of scenarios 2 and 3, "any action taken against [non-State actors] may raise issues about violating the sovereignty of that nation and its rights and obligations with respect to terrorist operations from or through its territory." OWENS ET AL., *supra* note 3, at 274.

means to suppress the threat; and (5) evaluate its prior interactions with the territorial State. Part III takes up these factors and applies them in the context of cyber attacks.

III. APPLYING THE TEST'S FACTORS TO CYBER ATTACKS

A. Preference for consent or cooperation

In the ideal situation, a victim State will approach the territorial State and inform the latter of the fact of the imminent or actual armed attack and its reasons for believing that the attacker is employing the victim State's infrastructure to commit the attacks. It then will seek consent to take action (whether forcible or not) to suppress the attacks emanating from the territorial State's computer systems. When it acts pursuant to and consistent with that consent, the victim State will not violate Article 2(4) of the Charter or the customary principle of non-intervention. Examples of such consent are not hard to find, particularly outside the cyber realm: Iraq previously allowed Turkey to use force in Iraq against a Kurdish terrorist group (the Kurdistan Workers' Party), and the United States reportedly is using force in Somalia and Yemen against members of Al Qaeda and associated forces with the consent of those governments.[26] Even if the territorial State is reluctant to let the victim State operate alone in its computer systems, there may well be opportunities for the two States to work cooperatively to suppress the threat.

This approach has several advantages. First, it minimizes the chance of cyber clashes between the victim and territorial States, and reduces the likelihood that those States find themselves working at cross-purposes against the cyber attacker. Second, this type of cooperation has the potential to enhance the victim State's own operations, to the extent that the territorial State has a deeper knowledge of its own computer systems, relationships with private sector companies whose computers the attacker may be using to facilitate the attack, and relevant information about past penetrations into the victim (or territorial) State's systems. Third, this cooperation and the corresponding information that it receives from the territorial State may help the victim State limit the collateral damage from its response, a

26. Scott Shane, *Yemen Sets Terms of a War on Al Qaeda*, NEW YORK TIMES, Dec. 4, 2010, at 1; U.S. Department of State Cable 09 NAIROBI 1057 ("Somalia TFG Prime Minister Worried About Rival") (Somalia).

constant concern in the cyber context.[27] The advantages of cooperation here may be more modest than in the more traditional context in which non-State actors conduct physical attacks against the victim State, however. In that context, local knowledge about terrain, terrorist camp locations and politics may prove particularly helpful in addressing the kinetic threats posed by terrorist or rebel groups. One disadvantage to obtaining consent or cooperation is temporal: in many cyber cases, a State may need (or wish) to respond to an ongoing attack immediately, leaving no time to seek a cooperative approach with the territorial State. One way to mitigate this temporal concern, while also promoting cooperation between the territorial and victim States, would be to negotiate consent agreements in advance.[28] In these agreements, the territorial State could provide advance consent to victim State operations in the former's cyber networks when certain triggers are met.

At the same time, the anonymity of cyber activity and the ease with which an actor may cover his tracks may reduce the victim State's overall incentives to seek any type of consent or cooperation from the territorial State before penetrating its cyber systems. In the cyber context, the victim State's actions in redress are less likely to come to light and, even if they do, it is easy for the victim State credibly to deny that it was the actual actor in that case.[29] In the non-cyber context, it is difficult (though not impossible) for a victim State physically to penetrate and use force in a territorial State without being detected. For example, an international investigation into the Cheonan incident (in which North Korea torpedoed a South Korean Navy ship) readily revealed Korean markings on the torpedo fragments.[30] In addition, the territorial State may be reluctant to cooperate with the host State

27. *See, e.g.*, Nakashima, *supra* note 5 (discussing U.S. concerns that actions in another country's networks could result in unintended consequences, including the disruption of civilian networks).

28. By way of precedent, the United States has negotiated a number of bilateral agreements relating to operations and ship-boarding to suppress the movement of narcotics and weapons of mass destruction. The latter set of agreements provides advance consent for either party to board a vessel flagged to the other party if the vessel is suspected of carrying illicit shipments of weapons of mass destruction. *See, e.g.*, Emma L. Belcher, *The Proliferation Security Initiative: Lessons for Using Nonbinding Agreements*, COUNCIL ON FOREIGN RELATIONS SPECIAL REPORT (July 2011).

29. *See* OWENS ET AL., *supra* note 3, at 81 (noting that most cyber attacks are inherently deniable).

30. Letter from the Permanent Representative of the Republic of Korea to the United Nations Addressed to the President of the Security Council (S/2010/281), June 4, 2010.

for national security reasons, particularly where the territorial State does not want to disclose information about its networks, systems and technology.

From a legal perspective, obtaining consent is an ideal way to avoid having to answer the host of difficult legal questions that currently attach to offensive and defensive uses of cyber tools. Action pursuant to consent also makes it less important that the victim State have a firm sense of who the author of the attacks is, because the territorial State is less likely to challenge the victim State's actions. From a political and military perspective, however, the costs of acting without seeking territorial State consent appear far lower than in the non-cyber context.

B. Request to address the cyber attack

Assume that the territorial State has not affirmatively consented to the victim State's use of cyber (or kinetic) tools to suppress the cyber threat emanating from the territorial State, perhaps because it is concerned about allowing the victim State to access its computer networks. At this point, the most direct way for a victim State to assess the territorial State's willingness and ability is to ask it to terminate the threat. Not only will this clearly put the territorial State on notice of the cyber attack, but it also will place an onus on the victim State to share relevant intelligence about the attack. If the territorial State responds by providing a plan for suppressing the attack, the victim State then has the basic information it needs to begin to assess the territorial State's willingness and ability to act.

Governments almost certainly will demand a caveat to this requirement, however. Where the victim State believes that the territorial State is colluding with the author of the cyber attack or will tip off the cyber attacker, the victim State should not be obligated to ask the territorial State before taking measures in the territorial State. This is a serious concern with States such as Russia and China, which are reported to use civilian proxies to conduct cyber attacks.[31] It is a particular concern in the cyber context because a hostile actor tipped off by the territorial State easily may divert its attacks through a different third State. Doing so in the non-cyber context takes time and money and poses significant logistical challenges.

31. Paul Rosenzweig, *From Worms to Cyber War*, DEFINING IDEAS, Dec. 9, 2011, http://www.hoover.org/publications/defining-ideas/article/102401 (describing Russian "cyber patriots"); David E. Sanger, John Markoff & Thom Shanker, *U.S. Plans Attack and Defense in Web Warfare*, NEW YORK TIMES, Apr. 28, 2009, at A1.

Creating too robust a caveat to the requirement to request assistance, however, will erode the balance that the "unwilling or unable" test strikes by putting a heavy finger on the scales in favor of security over sovereignty.

Even where the victim State is not concerned about a link between the territorial State and the hostile cyber actors, this factor magnifies complications that already exist in the non-cyber context. For the victim State, a requirement that it inform the territorial State about the cyber attacks it is suffering is not onerous. However, if the territorial State seeks additional information about those attacks—Are you sure they are coming from our territory? How do you know? What cyber tools do you have that can detect that, and how reliable are they?—the victim State may be hesitant to reveal its technological capacities.[32] Consider the territorial State's point of view as well. If the victim State simply asks it to suppress the threat, without seeking information about how the territorial State will do so, the territorial State may willingly comply, without having to reveal its cyber tools to the victim State. If the victim State seeks technological details about how the territorial State plans to proceed (which it reasonably might do to assure itself that the attacks will stop), the territorial State may be loath to reveal those details.[33] In the non-cyber context, it is far more likely that States will have adequate intelligence about each other's military hardware and capabilities. In the cyber context, the political relationship between the victim and territorial States—and, concomitantly, their willingness to share intelligence and technology—becomes highly predictive of how the victim State will proceed.

C. Good faith assessment of territorial State control and capacity

In the non-cyber world, when analyzing a territorial State's ability to suppress the threat, a victim State should assess what level of control the territorial State has over the geographic area from which the attacks are emanating. Conventional attacks plotted and launched from within a capital city may be far easier to detect, locate and suppress than attacks launched from remote jungles far from any town. A related question goes to the capacity of the territorial State's law enforcement and military officers, and

32. *See* Matthew Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421, 425 (2011) ("[N]o governments speak in much detail about their cyberwarfare capabilities and strategies at this point.").

33. As States garner increasing amounts of intelligence on each other's capabilities, this concern may diminish.

whether there are any reasons that those actors would not be able (or willing) to act against the non-State actors. In the cyber context, the question becomes how technologically sophisticated is the territorial State? While it is possible that one or more hostile actors is physically present in the territorial State, it is more likely that those committing cyber attacks against the victim State are present only electronically in the territorial State. Stopping those attacks, therefore, depends both on the capacity of the territorial State's cyber gurus and on the attacker's level of technical sophistication.

There is not enough publicly available information to gauge how often a victim State is likely to encounter a territorial State that is technically unable to defeat a cyber attack against the victim State. Some reports suggest that cyber is the great equalizer, allowing States with far weaker conventional militaries to take on those with traditionally strong conventional militaries.[34] Others assert that the cyber capacities of States such as the United States, Russia and China far exceed those of most other States.[35] Putting aside the objective capabilities of a particular territorial State, the secondary question of how much the victim State knows about the territorial State's capabilities remains a tricky one as long as cyber-capacities remain closely-held secrets. Publications such as *Jane's Defence Weekly* (as well as a State's domestic intelligence reports and the fact that States such as the United States may have provided weapons and training to the territorial State in question) make it relatively easy to ascertain what a State's kinetic capabilities are. In the cyber context, though, it will be particularly challenging for a victim State to assess the control and capacity of another State with which it does not have a close relationship already.

D. Good faith assessment of the territorial State's proposed means to suppress threat

Closely related to an assessment of the territorial State's capacity and control is a good faith assessment of the proposed means by which the territorial State will suppress the threat. The victim State must assess those pro-

34. Waxman, *supra* note 32, at 451, 455 (noting that "some experts assess that the United States is currently strong relative to others in terms of offensive capabilities" but also that "some States that are developing offensive cyber-warfare capabilities (such as North Korea, according to many experts) are non-status-quo powers or aspiring regional powers").

35. Leon Panetta, U.S. Secretary of Defense, Remarks on Cybersecurity (Oct. 11, 2012) ("It's no secret that Russia and China have advanced cyber capabilities."), http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

posed actions objectively. Even if the victim State would prefer to act itself, it should accept the territorial State's proposed approach if a "reasonable State" would believe that the approach will accomplish the victim State's core goal of suppressing the attack or threat of imminent attack.

In the non-cyber context, weeks may elapse between the time a territorial State proffers an operational plan and the time it executes it. In contrast, there will be almost immediate feedback on the success or failure of the territorial State's efforts to suppress the cyber threat. This makes it even more reasonable to defer to the territorial State's plan in the first instance, unless the ongoing attack against the victim State is so significant that there is no time for trial and error.

Establishing a preference for the territorial State's proposal is not without costs. Assume the territorial State proposes simply to shut off the server that is hosting the attacks against the victim State. Assume further that, if the territorial State permitted the victim State to address the threat itself, the victim State could stop the attack in a way that would allow it to continue to gather intelligence about the attacker. Should we continue to favor the territorial State's reasonable plan, even where doing so may force the victim State to lose some modicum of intelligence about its attacker? Probably so, though reasonable minds may disagree. What if the territorial State's plan is reasonable but is likely to result in some level of collateral damage, while the victim State has a high level of certainty that its plan would produce no such damage? In that case, the victim State would have at least a credible argument that the territorial State was "unable" to suppress the threat in a responsible way. Difficult questions such as these abound.

E. Prior interactions with the territorial State

Finally, in assessing the territorial State's proposed means to address the threat itself, the victim State should consider past interactions with the territorial State. Has the territorial State previously suppressed threats (conventional or cyber) emanating from its territory? Has the territorial State revealed a level of technical competence in the past that should give the victim State comfort that its proposed approach will work this time? Is the territorial State one from which cyber attacks consistently emanate, or is this an unusual incident? The more historically reliable and responsive the territorial State is, the less justification the victim State will have if it choos-

es to take action itself, and the more difficult it will be for the victim State to defend its actions if they come to light.

IV. ADVANCING CYBER LAW?

The United States has asserted that it will treat hostile acts in cyberspace as it would "any other threat to our country" and that it reserves the right to employ a military response, "as appropriate and consistent with applicable international law."[36] In other statements, the United States has made clear that in the non-cyber context, international law allows the United States to use force against non-State actors in another State's territory only when the territorial State has consented or is unwilling or unable to suppress the threat.[37] This—coupled with multiple news reports about internal debates within the U.S. government on cyber questions[38]—suggests that the United States is attempting to reason by analogy from existing international law governing the *jus ad bellum*. These reports also suggest that the United States is attempting to craft appropriate, and apparently highly restrictive, operational rules of the road in the cyber sphere. One news report stated that U.S. officials are focused on "concerns that action in another country's networks could violate international law, upset allies or result in unintended consequences, such as the disruption of civilian networks."[39] The article further reported that the U.S. Department of Defense has developed "strict conditions governing when military cyber-specialists could take action out-

36. THE WHITE HOUSE, U.S. INTERNATIONAL STRATEGY FOR CYBERSPACE 14 (May 1, 2011); Harold Koh, "International Law in Cyberspace," USCYBERCOM Interagency Legal Conference, Sept. 18, 2012.

37. Brennan, *supra* note 23 ("The United States does not view our authority to use military force against al-Qa'ida as being restricted solely to 'hot' battlefields like Afghanistan. Because we are engaged in an armed conflict with al-Qa'ida, the United States takes the legal position that—in accordance with international law—we have the authority to take action against al-Qa'ida and its associated forces without doing a separate self-defense analysis each time. And as President Obama has stated on numerous occasions, we reserve the right to take unilateral action if or when other governments are unwilling or unable to take the necessary actions themselves.").

38. *See, e.g.*, Nakashima, *supra* note 5; Ellen Nakashima, *Cyber-Intruder Sparks Massive Federal Response and Debate Over Dealing with Threats*, WASHINGTON POST, Dec. 8, 2011.

39. Nakashima, *supra* note 5. It is not clear whether those contemplated U.S. actions would be forcible or would consist of actions short of force (such as non-forcible countermeasures).

side U.S. networks" and that those conditions "are so stringent that the new capability to go outside military boundaries might never be used."[40]

In some ways this U.S. process is puzzling. In the face of such legal and technological uncertainty, one might expect a country with extensive cyber capabilities to take a minimalist approach to legal compliance, at least until the international community formulated certain common understandings about how to approach cyber warfare. Indeed, in the non-cyber context, the U.S. Government has done less hand wringing about using force extra-territorially, even though the manifestation of that force is far more public. Why is the United States working so hard to find the law and apply it in the cyber realm, where violations of Article 2(4) would be both legally uncertain and difficult to detect?

There are at least five factors that may explain why the United States has been edging cautiously toward a relatively constraining legal regime (one that in all likelihood will be a unilateral approach for some time to come). First, there often is an inherent institutional instinct in the U.S. government to anchor novel legal situations in existing bodies of law and practice, and to reason by analogy. This is, after all, the approach the Obama administration took toward detainee habeas cases.[41] There, the government determines (and asks courts to affirm) that someone is a combatant based on functional analogies between that person's activities and the activities of a member of a State's armed forces. Particularly where the analogies are quite reasonable (as they are between kinetic and cyber activities), it often is easier to draw from existing rules than to craft new ones from whole cloth. Additionally, U.S. government lawyers know that other governments are

40. *Id.* (noting that shutting down a server in another country likely would require Presidential permission). *See also* David Sanger, John Markoff & Thom Shanker, *U.S. Steps Up Effort on Digital Defenses*, New York TIMES, Apr. 27, 2009 (stating that President Bush personally authorized penetration by the U.S. military of a computer in Iraq to lure Al Qaeda members into an ambush); Ellen Nakashima, *Pentagon Considers Preemptive Strikes as Part of Cyber-Defense Strategy*, WASHINGTON POST, Aug. 28, 2010 (reporting on internal U.S. government debate about when the United States may go into foreign cyberspace and take preemptive action).

41. Respondent's Memorandum Regarding the Government's Detention Authority Relative to Detainees Held at Guantanamo Bay, In re: Guantanamo Bay Litigation, Mar. 13, 2010 (stating that the President has the authority under the 2001 Authorization for Use of Military Force to detain those persons whose relationship to Al Qaeda or the Taliban would, in appropriately analogous circumstances in a traditional international armed conflict, render them detainable).

likely to use those existing rules as a starting point from which to evaluate U.S. action.[42]

As a related matter, the U.S. culture surrounding the use of force and the conduct of armed conflicts has grown increasingly legalistic in the past ten years. While the United States always has been conscious of the legal role that the UN Charter plays in regulating uses of force, the past decade has found lawyers playing a particularly prominent role in structuring government decision making in this area.[43] A robust interagency process within the National Security Council ensures a forum for voices (such as those from the State Department) that are concerned about the diplomatic and reputational impacts of cyber activities that are seen as unlawful or illegitimate. And a perennial interest in being seen as following the rule of law renders unappealing an approach that ignores legal constraints entirely.[44]

Third, the United States is keenly aware of the ongoing controversy about its geographic approach to the U.S. conflict with Al Qaeda and associated forces.[45] The notion that the United States takes a forward-leaning approach to using force in third States with which it is not in conflict remains uncomfortable and legally contentious for many States. It follows that the United States would be similarly attuned to the far greater number of States that may (advertently or inadvertently) host cyber attacks against it, and to the almost-certain controversies that would follow from its uses of cyber (or kinetic) force in those States, absent a robust and well-articulated legal defense of those actions. Developing cautious standards through a cautious process is one way to establish that defense and to place other States on notice of its contents.

---

42. Matthew Waxman suggests that this is not the only approach that the United States might have taken. Waxman, *supra* note 32, at 453 (noting that it might be "in the United States' strategic interest to legally *delink* cyber-activities from armed force instead of defining force by reference to effects").

43. For a discussion of the role of international law in the Cuban Missile Crisis, *see* ABRAM CHAYES, THE CUBAN MISSILE CRISIS (1974). For the lawyers' role in the past ten years, *see* JACK GOLDSMITH, POWER AND CONSTRAINT xv (referring to "faceless executive-branch lawyers" micromanaging national security decisions).

44. Brennan, *supra* note 23 (describing one of the core values of the United States as "adhering to the rule of law").

45. *Id.* ("An area in which there is some disagreement is the geographic scope of the conflict. The United States does not view our authority to use military force against al-Qa'ida as being restricted solely to 'hot' battlefields like Afghanistan. . . . Others in the international community—including some of our closest allies and partners—take a different view of the geographic scope of the conflict, limiting it only to the 'hot' battlefields.").

Even assuming these three propositions are true, this does not explain why the United States has not chosen to adopt freedom of action in cyberspace—at least for now, while the law is very unclear and it remains difficult to attribute a particular cyber action to any particular actor. That is, if the United States felt that it were justified in responding to a particular incoming attack—even one with origins in a friendly and technologically advanced State—why would it not simply respond to the attack in that friendly State and then deny knowledge of the response? One answer seems to lie in concerns about cyber collateral damage.[46] Past efforts to dismantle particular websites have resulted in unexpected disruptions of servers in various countries. For instance, when the U.S. military dismantled a Saudi web site in 2008, it inadvertently disrupted over 300 servers, including in Texas, Saudi Arabia and Germany.[47] The high likelihood of collateral damage (and the concomitant likelihood that such damage becomes public) may place significant pressure on a country such as the United States to set a prudentially high bar for using cyber force in other States' territories.[48]

Finally, reciprocity concerns echo loudly in the ears of U.S. policymakers and lawyers. Even though the United States rarely will find itself being accused by other States of being unwilling or unable to suppress a particular cyber threat, the United States should be interested in prioritizing consent wherever possible, to create an expectation that other States affected by cyber attacks emanating from the United States will approach the U.S. government in the first instance, before taking unilateral action against U.S. cyber infrastructure.[49] This is particularly true because the United States is viewed as a major source of cyber attacks, cyber exploitations and botnets.[50] It is not in the U.S. interest to allow other States to claim that

---

46. *See* OWENS ET AL., *supra* note 3, at 121–26 (describing difficulty in calculating accurately collateral damage from a cyber attack and describing damage assessment techniques for cyber attacks as "primitive").

47. Nakashima, *Preemptive Strikes*, *supra* note 40.

48. Note that this is true even if the United States is in an international armed conflict with State X and wishes to use cyber force against computers located within State X. Even that activity, which does not implicate the "unwilling or unable" test, may lead to collateral damage in third States.

49. It seems much more likely that a State would contemplate using unilateral cyber force against the United States than using unilateral kinetic force against it.

50. Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View* 7, HOOVER INSTITUTE, http://media.hoover.org/documents/FutureChallenges_Goldsmith.pdf (last visited Oct. 28, 2012).

there is a legal black hole regarding cyber uses of force or to be able to claim that the "unwilling or unable" test has no substantive or procedural content.

V. CONCLUSION

The "unwilling or unable" test remains a relevant proposition when a victim State suffers a cyber armed attack that is launched from the territory of a non-hostile State. Depending on the kinds of cyber activities that States treat as violating a neutral State's obligations and those that they treat as rising to the level of an armed attack, the international community will employ the test more or less frequently. The nature of cyber attacks—including the speed at which they occur—places pressure on the victim State to conduct both a rapid and accurate assessment of the territorial State's capabilities and political disposition. Cyber attacks also place pressure on the territorial State to reveal some of its technological capacity if it wishes to avoid having the victim State act in its stead. The relationship between the territorial and victim States will play an outsized role in the outcome of the "unwilling or unable" inquiry. Yet this inquiry stands between the victim State and a "global cyberwar on terror," and must be taken seriously.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

The Law of State Responsibility in Relation to Border Crossings: An Ignored Legal Paradigm

Louise Arimatsu

89 INT'L L. STUD. 21 (2013)

Volume 89 2013

The Law of State Responsibility in Relation to Border Crossings: An Ignored Legal Paradigm

Louise Arimatsu[*]

I. INTRODUCTION

This article revisits the law of State responsibility to ask whether, rather than invoking self-defense, there is a better way to conceptualize a State's violent engagement with a non-State actor[1] located in the territory of another State when the latter does not consent to foreign intervention and is itself unable or unwilling to stop the non-State actor from directing further attacks. In posing this question my intention should not be misinterpreted as one that seeks to identify a broader exception to the general prohibition on the use of force; in fact, it is quite the reverse. This article proposes a more legally coherent account of State practice that preserves an inter-State reading of self-defense. In that process, it offers *an* explanation for the recent statements by the International Court of Justice (ICJ) that seem to rule out the option of invoking self-defense under Article 51 of the UN Charter

* Associate Fellow with the International Law Programme, Chatham House (UK). Thanks to Hemi Mistry for research support on this project. The views expressed in this article are the sole responsibility of the author and do not reflect the view of the author's affiliations.

1. The term "non-State actor" denotes any entity with the capacity to launch an armed attack, be they organized armed groups, terrorist groups or rebels.

against non-State actors.[2] Although this stance by the ICJ has been criticized for not corresponding with the recent practice of States, if Article 51 cannot be invoked to justify the use of force against a non-State actor in the scenario described above, are there any existing laws which *would* permit States to cross an international border lawfully?

In Part II, I argue that there are good reasons for preserving the traditional reading of Article 51, which was designed exclusively to regulate relations among States. To support this position, I identify the inherent weaknesses (as well as the attendant risks) embedded in the views that have emerged in recent years to justify the use of force against non-State actors based in the territory of a State that is unable to prevent further attacks but is also unwilling to consent to the armed intervention by the State under attack.

In Part III, I explore further the argument that favors extending Article 51 to non-State actors to ask why the non-State actor's geographical location determines the applicability of the *jus ad bellum*. If the answer to this question is simply that the crossing of the border is game-changing, an explanation of why this is so is warranted. If, on the other hand, there is no compelling reason why this should be so, it raises an important question as to whether self-defense is the most coherent legal framework within which to conceptualize the use of force against non-State actors. And if this indeed *is* the case, how might a border be lawfully crossed?

In Part IV, I tentatively suggest that existing international law has the potential to provide a satisfactory legal framework within which to address these questions. In addition to the two codified exceptions to the prohibition on the use of force, there is a long tradition, demonstrated by consistent State practice, that the wrongfulness of a use of force can be precluded in one, and possibly two, other exceptional circumstances found in customary international law. International law has long recognized the right of a State to consent to the intervention of foreign armed forces to assist it in maintaining its internal security. Where the intervention is consensual,

2. *See* Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 139 (July 9) [hereinafter Wall Advisory Opinion]; Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶ 147 (Dec. 19) [hereinafter Armed Activities Judgment]. But see also Judge Kooijmans' Separate Opinion, ¶¶ 31–35, and Judge Simma's Separate Opinion, ¶¶ 7–13, in the *Armed Activities* judgment.

there is no violation of Article 2(4).[3] A second principle of international law that precludes the wrongfulness of an act that would otherwise be considered a violation of the law is the plea of necessity. I suggest that it is this customary international law principle that provides a far more coherent basis upon which to justify the use of force against the non-State actor located in the territory of another State that is unwilling to prevent further attacks.

I conclude by arguing that the conditions attached to necessity function to severely restrict its availability, more so than self-defense. Thus, the critics of current State targeting policy with respect to the members of organized armed groups (OAGs) in foreign territories are no more likely to be convinced on the facts that a robust case of necessity has been made out. However, by contrast to self-defense, invoking necessity to justify the use of force against an OAG in the territory of another State enables that State to cross a border lawfully if the requisite conditions are satisfied. For the State claiming the right to use force in such circumstances, there are further legal hurdles thrown up by *jus in bello* that must be overcome before its conduct is considered lawful.

II. SEVERING THE LINK BETWEEN STATE ATTRIBUTION FOR AN ARMED ATTACK

Constituted in the aftermath of the Second World War, the primary ambition of the United Nations Charter system, as exemplified by Article 2(4), was to prevent future war between States.[4] The contemporary law on the use of force is founded on the now customary international law prohibition[5] set forth in the Article, which states: "All members shall refrain in their international relations from the threat or use of force against the territorial integri-

---

3. OSCAR SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE 114 (1991). Consent functions to negate what is otherwise a wrongdoing.

4. The Preamble of the Charter opens with the declaration,

> We the Peoples of the United Nations determined to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind, . . . and for these ends to practice tolerance and live together in peace with one another as good neighbours, and to unite our strength to maintain international peace and security, and to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest, . . . have resolved to combine our efforts to accomplish these aims.

5. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 190 (June 27) [hereinafter Nicaragua Judgment].

ty or political independence of any state or in any other manner inconsistent with the Purposes of the United Nations."[6]

The negotiating history of the Charter reveals that Article 2(4) was "intended to be a comprehensive prohibition on the use of force by one State against the other"[7] and, as the text makes clear, the provision was only concerned with inter-State uses of force. The Charter recognizes two exceptions to this prohibition: enforcement actions as provided under Articles 39, 41 and 42; and the right of individual and collective self-defense, codified in Article 51. A decision by the Security Council to authorize the use of armed force under Article 42 is conditioned on a prior determination by the Council as to the existence of a "threat to the peace, breach of the peace, or act of aggression" (Article 39).[8] While an act of aggression by definition can *only* be committed by States,[9] there is nothing to preclude the former two situations arising as a consequence of violence by non-State actors.[10] In fact there is considerable State practice to show that civil war situations, particularly where there are trans-boundary effects, have often been determined as amounting to "a threat to the peace."[11]

Article 51, on the other hand, has traditionally been regarded as an inter-State right that could be invoked only in the event of "an armed attack" by another State. More specifically, the article provides, "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations." Although this provision was not intended to preclude armed attacks by non-State actors that were acting on behalf of a State, what the Charter regime did not foresee was the prospect of an "armed attack" by a non-

---

6. U.N. Charter art.2, para. 4.

7. Sean Murphy, *Terrorism and the Concept of "Armed Attack" in Article 51 of the U.N. Charter*, 43 HARVARD INTERNATIONAL LAW JOURNAL 41 (2002).

8. Article 41 is concerned with measures not involving the use of armed force that may be used to enforce a Security Council decision.

9. Declaration on the Definition of Aggression, G.A. Res. 3314, U.N. Doc. A/RES/3314 (Dec. 14, 1974).

10. As the commentary to Rule 18 of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* notes, the Security Council has also "labelled two significant phenomena as threats to the peace"—international terrorism and the proliferation of weapons of mass destruction. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., forthcoming 2013) [hereinafter TALLINN MANUAL].

11. S.C. Res. 1973, pmbl., U.N. Doc. S/RES/1973 (Mar. 17, 2011); S.C. Res. 1527, pmbl., U.N. Doc. S/RES/1527 (Feb. 4, 2004); S.C. Res. 1484, pmbl., U.N. Doc. S/RES/1484 (May 30, 2003); S.C. Res. 924, pmbl., U.N. Doc. S/RES/924 (June 1, 1994).

State actor acting without (or with minimal) State involvement. This was most probably because there was an assumption that armed attacks by such actors on the scale and gravity envisaged by Article 51 would *necessarily* involve a State. The attacks on 9/11 challenged that assumption, prompting a fundamental rethinking of the law on the use of force.

Three views now dominate the discourse on the applicability of Article 51 to armed attacks by non-State actors. The first insists on the preservation of a strong link between the non-State actor that launches an armed attack and a State (typically the territorial State from which such an attack is launched). In other words, Article 51 may only be invoked in situations where there is "substantial involvement" by a State in the armed attack carried out by the non-State actor. The second view attempts to extend to victim States a remedy in situations where there is little or no evidence of the territorial State's involvement in the armed attack although it has allowed its territory to be used a base from which the non-State actor is able to mount such an attack. Advocates of this view maintain that under such circumstances a victim State should be entitled to use force pursuant to Article 51 against the State that harbors or gives sanctuary to the non-State actor. Proponents of the third view simply claim that Article 51 applies to armed attacks by non-State actors. According to this view, the State from which the attack has been facilitated cannot claim that its territorial integrity or sovereignty has been violated if the victim State uses force in self-defense as long as the principle of necessity is strictly adhered to. Each of these views warrants further comment since there are inherent problems associated with all three.

Although the traditional view of Article 51 is founded on an inter-State conception of the right to use force, this stance has never absolutely precluded the applicability of the right of the victim State to use force in response to an armed attack by a non-State actor where there is "substantial involvement" by a State in that attack. This latter point was elaborated by the ICJ in the *Case Concerning Military and Paramilitary Activities in and Against Nicaragua* (*Nicaragua* judgment) when it was required to consider whether acts committed by the contras in the course of their military operations in Nicaragua could be attributed to the United States.[12] In that case the ICJ noted that "the sending by or on behalf of a State of armed bands, groups, irregular or mercenaries, which carry out acts of armed force against another State . . . or its substantial involvement therein" could amount to an

12. Nicaragua Judgment, *supra* note 5, ¶ 115.

armed attack within the meaning of Article 51 if the operation, because of its "scale and effects," would have been classified as an armed attack had it been carried out by regular armed forces of the State.[13] In other words, although force could be used pursuant to Article 51 in the event of an armed attack by non-State actors, the right to do so was preconditioned on the involvement of a State in that attack. The pivotal question turned on what *degree of involvement* by a State was necessary to enable a victim State to invoke self-defense.[14] According to the ICJ, the standard was high. For the conduct of irregular forces to give rise to legal responsibility on the part of the State, the non-State actor must have been in a relationship of "complete dependence"[15] or under the direction or "effective control" of a State.[16] Insofar as the ICJ was concerned, "general control" by the State or even a "high degree of dependency," including the financing, organizing, training, supplying or equipping of the non-State actor, did not suffice.[17]

The customary international law test for attributing the wrongful acts of non-State actors to a State is set forth in Article 8 of the International

---

13. *Id.*, ¶ 195.

14. According to Judge Schwebel, a State must at least exercise significant, perhaps determinative, influence over the non-State actor's decision making, as well as play a meaningful role in the specific operations before an armed attack will be imputed to it. *Id.*, ¶ 6 (separate opinion of Judge Schwebel).

15. In the *Nicaragua* judgment, the ICJ concluded there was insufficient evidence to demonstrate the contras' complete dependence on the United States and therefore it was unable to determine that the contra force could equated for legal purposes with the forces of the United States. *Id.*, ¶¶ 109–10. In the *Genocide* case, the ICJ upheld the "complete dependence" test and explained,

> [I]t is appropriate to look beyond legal status alone, in order to grasp the reality of the relationship between the person taking action, and the State to which he is so closely attached as to appear to be nothing more than its agent: any other solution would allow States to escape their international responsibility by choosing to act through persons or entities whose supposed independence would be purely fictitious. However, so to equate persons or entities with State organs when they do not have that status under internal law must be exceptional, for it requires proof of a particularly great degree of State control over them.

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), 2007 I.C.J. 108, ¶¶ 392–93 (Feb. 26) [hereinafter Genocide Case].

16. Nicaragua Judgment, *supra* note 5, ¶ 115. As elaborated by the ICJ in the *Genocide* case, the "complete dependence" test is fundamentally distinguishable on the basis that the non-State actor cannot be considered other than a de facto State organ and so "all [its] actions performed in such capacity would be attributable to the State for purposes of international responsibility." Genocide Case, *supra* note 15, ¶ 397.

17. Nicaragua Judgment, *supra* note 5, ¶ 115.

Law Commission's (ILC's) Articles on State Responsibility.[18] Partially relying on the *Nicaragua* judgment, Article 8 provides that "[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of that State in carrying out the conduct."[19] As the ILC notes, it is widely accepted in international jurisprudence that responsibility attaches to a State for the wrongful acts of non-State actors if the former has authorized the acts in question; thus, if, on the specific instructions of a State, a non-State actor launches an armed attack on another State, the State that issued the instructions will be held responsible for the wrongful conduct.[20] It follows that since the State which instructs the non-State actor to commit the wrongful act is legally responsible for the commission of that act, if the act amounts to an "armed attack," the victim State is entitled to respond in self-defense against the State despite the fact that the actual attack may have been carried out by the non-State actor. The more difficult cases are armed attacks that are ostensibly carried out "under the direction or control" of a State. But as the ILC suggests, "such conduct will be attributable to the State only if it directed or controlled the specific operation and the conduct complained of [i.e., the armed attack] was an integral part of that operation."[21] Accordingly, if a State has effective control over the non-State actor's military operation which is of such "scale and effects" that it cannot be classed as anything but an armed attack (as in the case of specific instructions) the victim State is entitled to resort to force in self-defense against that State although the attack itself may have been carried out by the non-State actor. In that the majority in the ICJ's 2004 advisory opinion on the *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territories* appeared to foreclose the possibility that an armed attack within the meaning of Article 51

18. JAMES CRAWFORD, THE INTERNATIONAL LAW COMMISSION'S ARTICLES ON STATE RESPONSIBILITY: INTRODUCTION, TEXT AND COMMENTARIES 110 (2002). The standard set forth in Article 8 relied on the test of attribution identified by the ICJ in the *Nicaragua* judgment. The conduct of non-State actors may also be attributed to a State under Article 11 if the State "acknowledges and adopts the conduct in question as its own."

19. *See also* Genocide Case, *supra* note 15, ¶¶ 398, 406.

20. *See* Nicaragua Judgment, *supra* note 5, ¶ 195; Armed Activities Judgment, *supra* note 2, ¶ 146. *See also* U.N. Definition of Aggression, G.A. Res. 3314 (XXIX), U.N. GAOR, 6th Comm, 29th sess., 2319th plen. mtg., U.N. Doc. A/RES/3314 (XXIX) (Dec. 14, 1974).

21. CRAWFORD, *supra* note 18, at 110, ¶ 3.

can originate from a non-State actor, the judgment is problematic, not least since such a scenario was expressly recognized in the *Nicaragua* judgment.[22] Nor can this stance be reconciled with State practice. Nevertheless, even the more fluid *Nicaragua* test has engendered its own set of problems because it insists on a direct correlation between the *jus ad bellum* and State responsibility legal regimes.[23]

The consequence of this is that the traditional inter-State approach fails to adequately provide a meaningful remedy for States that are subject to armed attacks by non-State actors in situations where: (1) there is inadequate proof to show that there is substantial involvement of a State in the attack; and (2), there is little or no involvement by a State in the armed attack although the State from where the attack was conducted allowed its territory to be used by the non-State actor.[24] The ICJ's faithful application of the test of attribution elaborated in the *Nicaragua* judgment to the facts before it in the case concerning *Armed Activities on the Territory of the Congo* (*Armed Activities* judgment) meant the ICJ could not *but* reject Uganda's claim that it had acted in self-defense.[25] With "no satisfactory proof" of the involvement of the Democratic Republic of Congo in the "armed attacks" by the rebel forces, Uganda was precluded from invoking Article 51, leaving it with no satisfactory remedy apart from countermeasures—in other words, measures short of force.[26] Although the traditionalists recognize that the State that allows its territory to be used by such groups is in violation of its customary international law obligations,[27] the best answer they

22. Wall Advisory Opinion, *supra* note 2, ¶ 139.

23. For useful analysis, see Nicholas Tsagourias, *Necessity and the Use of Force: A Special Regime*, 41 NETHERLANDS YEARBOOK OF INTERNATIONAL LAW 11 (2010).

24. SCHACHTER, *supra* note 3, at 169.

25. Armed Activities Case, *supra* note 2, ¶¶ 146–47. *But see also* Separate Opinion of Judge Kooijmans, ¶¶ 29–30, and Separate Opinion of Judge Simma, ¶ 12.

26. In the *Oil Platforms* judgment, Judge Simma took the position that proportionate countermeasures could involve a limited degree of military force in response to circumstances below the Article 51 threshold of "armed attack." Separate Opinion of Judge Simma, Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶¶ 12–13 (Nov. 6). Rosalyn Higgins, *A Babel of Judicial Voices? Ruminations from the Bench*, 55 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 795 (2006).

27. In the *Corfu Channel* case, the ICJ held that every State is obliged "not to allow knowingly its territory to be used for acts contrary to the rights of other states." Corfu Channel (U.K. v. Alb.) 1949 I.C.J. 4, ¶ 22 (Apr. 9). See also paragraph 4 of the Declaration on Friendly Relations. Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), U.N. GAOR, 25th Sess., Supp. No. 28, at 121, U.N.

can offer is to point to countermeasures and/or the law enforcement paradigm. But what they cannot do is to resolve the situation in which the territorial State that harbors the non-State actor is unwilling to prevent further attacks let alone detain, extradite or even prosecute such actors.[28]

This legal lacuna has been widely debated in legal journals since the 1980s prompting some to argue for a far more expansive interpretation of Article 51 than that set out in the *Nicaragua* judgment.[29] Proponents of this second view suggest that the State that harbors or allows its territory to be used by the non-State actor which engages in an armed attack is equally responsible for that wrongful act.[30] While this view has garnered far more support in the post-9/11 period, State practice prior to that point indicates that a narrow inter-State reading of self-defense prevailed.[31] Repeated attempts to extend the right of self-defense to encompass harboring (often equated to aiding and abetting)[32] the non-State actor were generally treated as inadequate bases upon which to claim the lawful use of force in self-defense. For example, in spite of Israel's assertion that "a country cannot claim the protection of sovereignty when it knowingly offers a piece of its territory for terrorist activity against other nations," its 1985 attack on the

---

Doc. A/8082 (1970). In the *Armed Activities* judgment the ICJ held General Assembly Resolution 2625 declaratory of customary international law and that "no State shall organize, assist, foment, finance, incite or tolerate subversive, terrorist or armed activities directed towards the violent overthrow of the regime of another State, or interfere in civil strife in another State." Armed Activities Judgment, *supra* note 2, ¶ 162. *See also* S.C. Res. 1373, U.N. Doc S/RES/1373 (Sept. 28, 2001).

28. Since the early days of the U.N. Charter, commentators have cautioned that any law "which prohibits resort to force without providing a legitimate claimant with adequate alternative means of obtaining redress, contains the seeds of trouble." C.H.M. Waldock, *The Regulation of the Use of Force by Individual States in International Law*, 81 RECUEIL DES COURS (Hague Academy of International Law) 455 (II-1952)

29. Abraham Sofaer, *Sixth Annual Waldemar A. Solf Lecture in International Law: Terrorism, the Law and the National Defense*, 126 MILITARY LAW REVIEW 89 (1989); Ruth Wedgwood, *Responding to Terrorism: The Strikes Against bin Laden*, 24 YALE JOURNAL OF INTERNATIONAL LAW 559 (1999).

30. A further problematic aspect of this view is that proponents sometimes refer to the State that harbors the non-State actor while others talk of the State from whose territory an attack is launched.

31. *See generally* Tom Ruys & Sten Verhoeven, *Attacks by Private Actors and the Right of Self-Defence*, 10 JOURNAL OF CONFLICT AND SECURITY LAW 289–320 (2005).

32. For a discussion on the flaws of equating "harboring" with the criminal law concept of "aiding and abetting," see Jules Lobel, *The Use of Force to Respond to Terrorist Attacks: The Bombing of Sudan and Afghanistan*, 24 YALE JOURNAL OF INTERNATIONAL LAW 537 (1999).

headquarters of the Palestinian Liberation Organization in Tunisia on the grounds that it was acting pursuant to Article 51 was rejected by the Security Council, with the United States abstaining.[33] What is more, none of the members of the Council appeared persuaded by the U.S. contention that "an aspect of the inherent right of self-defense recognized in the United Nations Charter [is that] a State subject to continuing terrorist attacks may respond with appropriate use of force to defend itself against further attacks."[34] Similarly, the U.S. strikes at sites in Afghanistan and Sudan in August 1998 following the Al Qaeda bombings of the American embassies in Kenya and Tanzania as justified exercises of self-defense received mixed reactions.[35] Caution is nevertheless required before reaching any conclusion as to the scope of the law since the reaction of States to many of these incidents during this period were clearly framed by political alignments. That said, State practice did not appear to deviate much from the interpretation of self-defense elaborated by the ICJ in the *Nicaragua* judgment.

Proponents of the second view nevertheless point to the conduct of States in the immediate aftermath of 9/11 as having fundamentally altered the traditional conception of Article 51. Security Council Resolutions 1368 (2001) and 1373 (2001) and subsequent State practice are cited as evidence for the emergence of an instant customary international law right favoring an expansive interpretation of self-defense.[36] Those who have long pressed for such an approach recall the widespread international support for Operation Enduring Freedom, which was launched in (and against) Afghanistan on the basis that the threat posed by Al Qaeda was "made possible by the decision of the Taliban regime to allow the parts of Afghanistan that it con-

33. For the exchanges between States, see U.N. SCOR, 40th Sess., 2615th mtg., U.N. Doc. S/PV.2615 (Oct. 4, 1985).

34. *Id.*

35. *See* letter dated 20 August 1998 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council invoking Article 51. U.N. Doc. S/1998/780 (Aug. 20, 1998). Britain, Germany, Australia, New Zealand and Israel supported the military operations; France and Italy were equivocal, while Russia, China, Pakistan, several Arab States and the Non-Aligned Movement were critical.

36. On the question of whether the case of Afghanistan represented the formation of instant custom or whether it ought to be regarded as an exception, see Antonio Cassese, *Terrorism is also Disrupting Some Crucial Legal Categories of International Law*, 12 EUROPEAN JOURNAL OF INTERNATIONAL LAW 997 (2001); Christine Gray, *The Use of Force and the International Legal Order*, *in* INTERNATIONAL LAW 604 (Malcolm Evans ed., 2003).

trols to be used by this organization as a base of operation."[37] Nevertheless, even supporters of the military action have conceded that justifying the use of force against *Afghanistan* is "a difficult question."[38]

State practice in the decade since 9/11 is marked by a certain degree of ambiguity.[39] For example, although the international community criticized Israel's use of force during its 2006 conflict with Hezbollah as being disproportionate, many supported its right to use force in self-defense.[40] Yet the issue over which there was palpable unease was whether such force could lawfully be used in *Lebanon* without violating its territorial sovereignty, not least because there was a belief that Iran and Syria, rather than Lebanon, were facilitating Hezbollah's military operations.[41] Although a majority of experts agree that mere harboring (or indeed the failure of a State to

37. Letter dated 7 October 2001 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council. U.N. Doc. S/2001/946 (Oct. 7, 2001). The UK also justified its military action in Afghanistan under Article 51 on the grounds that the Taliban regime was "supporting" Al Qaeda. U.N. Doc. S/2001/947 (Oct. 7, 2001).

38. CHRISTOPHER GREENWOOD, *International Law and the Pre-emptive Use of Force: Afghanistan, Al-Qaida and Iraq*, *in* ESSAYS ON WAR IN INTERNATIONAL LAW 684, 686 (2006). Greenwood dismisses the objections on the basis that "the criteria for determining the responsibility of a State for the acts of a private organisation are not altogether clear" and that since Afghanistan was in violation of international law in permitting Al Qaeda to operate from its territory, this "exposed its own forces to lawful attack in exercise of the right of self-defence."

39. Article 1(c)(xi) of the African Union Non-Aggression and Common Defence Pact, 2005, defines aggression to include "the encouragement, support, harbouring or provision of any assistance for the commission of terrorist acts and other violent transnational organized crimes against a Member State." See also Article 1(3)(k) of the 2006 Protocol on Non-Aggression and Mutual Defence in the Great Lakes Region.

40. For example, the UN Secretary-General stated, "While Hizbollah's actions are deplorable and, as I have said, Israel has a right to defend itself, the excessive use of force is to be condemned." U.N. SCOR, 61st Sess., 5492nd mtg., U.N. Doc. S/PV.5492 (July 20, 2006).

41. See Identical Letters dated 12 July 2006 from the Permanent Representative of Israel to the United Nations addressed to the Secretary-General and the President of the Security Council, which read, "Responsibility for this belligerent act of war lies with the Government of Lebanon, from whose territory these acts have been launched into Israel. Responsibility also lies with the Government of the Islamic Republic of Iran and the Syrian Arab Republic, which support and embrace those who carried out this attack." U.N. Doc. A/60/937-S/2006/515 (July 12, 2006). Revealingly, in his briefing to the Security Council the UN Secretary-General emphasized that "any analogy with Afghanistan under the Taliban is wholly misleading." U.N. SCOR, 61st Sess., 5492nd mtg., U.N. Doc. S/PV.5492 (July 20, 2006).

police its territory to prevent the launch of attacks) is insufficient to attribute the actions of non-State actors to the State for the purpose of finding a use of force by that State, many also share the view that the provision of sanctuary coupled with other acts, such as substantial support for the non-State group, could, in certain circumstances, be considered a use of force.[42] Advocates of the second view are not insensitive to the inherent risks associated with their position, since lowering the threshold of attribution necessarily increases the possibility of armed conflict.[43] But the case of Lebanon also exposes a far more problematic aspect of the second view in that the reasoning upon which self-defense rests is implicitly being reconfigured.

As an exceptional measure of self-help, self-defense is traditionally understood to operate to negate an otherwise wrongful act (the use of force by the victim State) in response to a prior wrongdoing (an armed attack) for the purpose of preventing further wrongdoing (attacks) by the *perpetrator* of the original wrong. Structurally, the plea regulates the conduct between two parties: the aggressor and the victim of that aggression. Additionally, it implicitly introduces a temporal limitation on the use of force in that once the aggressor no longer has the ability to conduct armed attacks, there is no further need—and by implication, requirement—for the victim to use defensive force. In its revised form, self-defense is being stretched to breaking point on both counts. Insofar as the temporal limitation is concerned, it is difficult to identify at what point the victim State need no longer use defensive force since self-defense was invoked against the party that was not directly responsible for the original armed attack.[44] Second, on this reading, self-defense is required to negate an otherwise wrongful use of force against the State that *harbors* the non-State actor, rather than against the *perpetrator of the armed attack*. The only way to resolve this incongruity is to accept, as some claim, that no distinction should be drawn between the two.[45] There will of course be some cases when the State from whose terri-

---

42. *See* Definition of Use of Force, TALLINN MANUAL, *supra* note 10, commentary to Rule 11, ¶ 5.

43. *See* Claus Kress, *Some Reflections on the International Legal Framework Governing Transnational Armed Conflicts*, 15 JOURNAL OF CONFLICT AND SECURITY LAW 245, 247–251 (2010).

44. Does defensive force end when the non-State actor is no longer able to conduct attacks from the territory of that particular State or from any other, or when the State no longer harbors such actors?

45. See, for example, the United States' *National Security Strategy* (Sept. 2002) and the 9/11 COMMISSION REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 326 (2004). The UK Attorney-General in a statement to the

tory the attack has been launched has played an active role in facilitating the attack; however, that will not always be the case, as was aptly demonstrated by the Lebanon example. The unease associated with this bind often translates into public statements by those claiming self-defense to emphasize that the use of force is directed not at the territorial State but the offending non-State actor. This unsatisfactory situation has thus given rise to a third view that calls for Article 51 to be extended to armed attacks by non-State actors.

According to this view, a victim State should be entitled to resort to defensive force against a non-State actor as long as the *Nicaragua* "scale and effects" test is satisfied.[46] The fractious attribution question is thereby completely by-passed since there is no need to attribute the armed attack to any State, including the one from which the armed attack was launched.[47] In support of this view proponents point to State practice in the immediate wake of 9/11 which recognized the inherent right of States to use defensive force in response to attacks by non-State actors.[48] This view is further strengthened by the silence in the primary legal texts, which make no express reference to an armed attack having to originate from a State,[49] a con-

---

House of Lords on April 21, 2004 stated, "[F]orce might, in certain circumstances, be used in self-defence against those who plan and perpetrate [terrorist] acts and against those harbouring them, if that is necessary to avert further such terrorist acts." 21 Apr. 2004, PARL. DEB., H.L. (2004) 356 (Lord Thomas of Gresford, statement opening the debate on international self-defense), http://www.publications.parliament.uk/pa/ld200304/ldhansrd/vo040421/text/40421-07.htm.

46. It should be noted that there is a tendency among proponents of this view to conflate the *jus ad bellum* with the *jus in bello* rules; for example, the *jus ad bellum* "scale and effects" test is often equated to the *jus in bello* "intensity" threshold. Kress, *supra* note 43.

47. YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 206–8 (4th ed. 2005); Murphy, *supra* note 7; Ken Anderson, *Targeted Killing and Drone Warfare: How We Came to Debate Whether There Is a "Legal Geography of War"* 7 (WCL Research Paper No. 2011-16, 2011), *available at* http://ssrn.com/abstract+1824783 (last visited Oct. 2, 2012).

48. As with the second view, evidence cited includes Security Council Resolutions 1368 and 1373 and NATO's invocation of Article 5 of the Washington Treaty, which states that an armed attack against one or more of the Allies in Europe or North America "shall be considered an attack against them all." North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243, a*vailable at* http://www.nato.int/cps/en/natolive/official_texts_17120.htm [hereinafter Washington Treaty].

49. This evidence is not as equivocal as advocates maintain. For example, Article 3(1) of the 1947 Inter-American Treaty of Reciprocal Assistance states that the High Contracting Parties

> agree that an armed attack by any State against an American State shall be considered as an attack against all the American States and, consequently, each one of the said Contract-

sideration that did not go unnoticed by some of the ICJ judges in the *Wall* advisory opinion and in the *Armed Activities* judgment.[50]

The right to use defensive force against a non-State actor pursuant to Article 51 is tempered by the principles of necessity, proportionality, and imminence of the attack. The principle of necessity is required to play a far more prominent role in the context of defensive force against non-State actors than it does in the case of inter-State defensive force. This is so in two respects. First, embedded in the inter-State conception of defensive force is a fidelity to the territorial border, which functions to confine the force that may be deployed to specific geographical locations. This is achieved through the implicit recognition that when inter-State force is used, the territories of States *not* party to the conflict remain undisturbed, protected by the principle of territorial sovereignty. Extending self-defense to non-State actors severs the link with this geographical constraint (for the simple reason that the non-State actor is not defined by any territorial attributes), introducing the prospect of borderless wars. The principle of necessity performs a critical role by reintroducing a spatial limitation to self-defense, insisting that it is only if the State that harbors is unwilling or unable to respond in an appropriate manner to prevent further attacks that defensive force is lawful. Second, it would appear that the principle of necessity functions to preclude the territorial State from insisting that its territorial sovereignty be respected, possibly on the basis that it is in violation of its international obligation not to allow its territory to be used as a base from which attacks can be conducted.

To extend Article 51 to armed attacks by non-State actors seems to offer a simple solution insofar as the relationship between the non-State actor and the State that is the target of the armed attack is concerned. However, this view raises a number of derivative questions. Why does the geograph-

---

> ing Parties undertakes to assist in meeting the attack in the exercise of the inherent right of individual or collective self-defence recognized by Article 51 of the Charter of the United Nations.

Inter-American Treaty of Reciprocal Assistance Between the United States of America and Other American Republics, Sept. 2, 1947, 62 Stat. 1681, 21 U.N.T.S. 77, a*vailable at* http://www.state.gov/p/wha/rls/70681.htm. However, neither Article 51 of the UN Charter nor Article 5 of the Washington Treaty includes an express reference to States, with the latter merely providing that "an armed attack against one or more of the Allies in Europe or North America shall be considered an attack against them all." Washington Treaty, *supra* note 48.

50. *See, e.g.*, Wall Advisory Opinion, *supra* note 2, Declaration of Judge Buergenthal, ¶ 6; Separate Opinion of Judge Kooijmans, ¶ 35; Separate Opinion of Judge Higgins, ¶ 33.

ical location of the non-State actor determine whether or not the State must justify its use of force? *Should* the location of the non-State actor determine the legal relationship between it and the State?

III. CROSSING THE BORDER

That States have willingly consented to limit their right to use force in accordance with the *jus ad bellum* does not impinge or alter in any manner the premise that the legitimate use of force rests exclusively with the State.[51] Nor has the acceptance for greater international regulation of the violence between State and non-State actors had any bearing on the fact that it is *only* the State that is entitled to lawfully resort to force. The right to *use* force thus continues to be jealously guarded by States as a sovereign prerogative recognized by international law and enforced in accordance with domestic law. To the extent that non-State actors engage in unauthorized violence within a State (in other words, violence without the lawful authority of the State) they will be treated as criminals under domestic law regardless of whether the situation of violence amounts to an armed conflict.[52] It is the fact that the non-State actor has taken up arms without lawful State authority that extends to the State the right to use force to suppress the violence. The degree of force that may be wielded by the State is context dependent and contingent on what legal regime applies in the circumstances. Experts may disagree on what *level* of force is appropriate in any given situation (whether the force is proportionate) but the issue over which there is no disagreement is that the territorial State is not required to justify its *use* of force whether as a law enforcement exercise in peacetime or a military operation in an armed conflict situation. In neither case is Article 51 relevant.[53]

As already noted, self-defense is an exceptional right raised by a State to justify its *use* of force. It is therefore somewhat incongruous that a State should be required to justify its use of force against a *non-State actor* that has

---

51. Max Weber defined a State as "a human community that (successfully) claims the *monopoly of the legitimate use of physical force* within a given territory." Max Weber, *Politics as Vocation*, *in* ESSAYS IN SOCIOLOGY 78 (2001).

52. All States have legal frameworks which privilege their own police and armed forces over insurgents who oppose them. Dieter Fleck, *The Law of Non-international Armed Conflicts, in* THE HANDBOOK OF INTERNATIONAL LAW OF MILITARY OPERATIONS ¶ 1202.2 (Dieter Fleck & Terry D. Gill eds., 2008).

53. DINSTEIN, *supra* note 47, at 204.

engaged in violent activities directed against that State merely because the non-State actor is located on the territory of another State when no such justification would be expected were that same non-State actor to be located within the State's own territory. Dinstein's explanation for this is that "an armed attack against a State, in the meaning of Article 51, posits some element external to the victim State. Non-State actors must strike at a State from the outside."[54] Yet this still does not fully explain why the location of the non-State actor, or the crossing of a border, fundamentally alters a pre-existing relationship. This may account for the ambiguity that surrounds State practice, which is overshadowed by a deep-seated disquiet insofar as justifying the use of force against a non-State actor is concerned. The question that cannot be avoided is whether the geographical location of the non-State actor should, as a matter of law, alter the legal relationship between the State and non-State actor, let alone determine the applicability of the *jus ad bellum*. To answer in the affirmative is evocative of the claim held not long ago that the location of an armed conflict determines the classification of that conflict, revealing, if nothing else, the extent to which geography frames perceptions.

If there is no compelling reason why the non-State actor's location should be determinative, self-defense may not necessarily be the most coherent legal framework within which to conceptualize the use of force against such actors. If this is indeed the case, how might a border be lawfully crossed by a State without violating the territorial sovereignty of the State in which force is deployed? History is replete with examples of non-State actors attacking States from the territory of another State. The capacity of such actors to "wage war" against a State may have increased but the problem is not new. Did the Charter create a normative framework leaving States with no remedy? Is there a legal vacuum that must be filled?

The UN Charter may have introduced a legal regime which codified two exceptions to the prohibition on the use of force, but there is a long tradition, demonstrated by consistent State practice, that the wrongfulness of a use of force can be precluded in one, and possibly other exceptional circumstances found in customary international law. In the event that the territorial State is unable to prevent further attacks from its territory, international law does not prohibit it from inviting foreign forces onto its territory to stop the attacks,[55] as long as the consent is regarded as "valid" and

54. *Id.* at 204–5.

55. The question of what legal regime applies to the foreign armed forces is a separate matter and must be determined on a case-by-case basis.

does not involve the violation of a peremptory norm. This principle is set forth in Article 20 of the Articles on State Responsibility.

As already noted, *primary* legal responsibility for prevention resides with the State from which such attacks have been conducted.[56] Nevertheless, in situations where the territorial State is unable to prevent further attacks yet is unwilling to consent to foreign intervention, the customary international law plea of necessity, I suggest, provides a far more coherent basis upon which to justify the use of force rather than self-defense. Such a suggestion is likely to court considerable criticism and resistance not least because necessity often arouses great angst. The unease is not without foundation since all exceptions threaten the rule.[57] Nevertheless, the concern that "in practice and over time the threshold for necessity will atrophy or 'soften'"[58] is one that is perhaps overstated and should not serve as the basis for rejecting a more lucid approach to the law. That a normative gap in respect of non-State actors was created by the UN Charter regime is unsurprising since the objective of the drafters was to design a legal framework to regulate the relations between States. Attempts to remedy the gap in the law have to date focused on Article 51 but, as discussed above, there are intrinsic problems with each of the proposals suggested. Rather than stretching Article 51 beyond recognition, necessity, as set forth in Article 25 of the Articles on State Responsibility, may offer a better option in that it has the capacity to fill the void on a far more robust footing.

IV. THE PLEA OF NECESSITY

Despite the evidence supporting the customary international law plea of a "state of necessity" there has been little discussion as to its potential relevance and value in resolving the current legal quandaries facing States in their violent exchanges with non-State actors located in another State.

---

56. The nature of the attack may, however, alter this assumption. A more coherent view mandates that it is not the territory from which an attack is launched but the territory in which the non-State actor that is responsible for the attack is situated that matters.

57. As Crawford observes, "[T]he commentary admits that scholarly opinion on the plea of necessity is sharply divided, suggesting that a further reason for this was the earlier tendency to abuse the doctrine of necessity to cover cases of aggression, annexation or military occupation." James Crawford, Special Rapporteur, Second Report on State Responsibility, ¶ 278, Int'l L. Comm'n, 51st Sess., U.N. Doc. A/CN.4/498/Add.2 (Apr. 30, 1999) [hereinafter Crawford Second Report].

58. Robert Sloane, *On the Use and Abuse of Necessity in the Law of State Responsibility*, 106 AMERICAN JOURNAL OF INTERNATIONAL LAW 447, 502 (2012).

Those who have entertained the possible relevance of the plea are quick to dismiss it as not applicable to situations that involve the use of force, although this view is not shared by all.[59] Simply put, necessity denotes a situation in which a State whose sole means of safeguarding an essential interest adopts conduct not in conformity with what is required of it by an international obligation to another State. But because the harm it faces is imminent and serious, along with the fact that any other course of conduct is likely to result in even more serious consequences, no State responsibility is incurred for the violation. Although not commonly invoked, the customary status of necessity was expressly recognized by the ICJ in the *Gabcikovo-Nagymaros Project* case when, after having carefully weighed the submissions by the parties and in light of the reports by the ILC, the ICJ held that "the state of necessity is a ground recognized by customary international law for precluding the wrongfulness of an act not in conformity with an international obligation."[60] Similarly, in the *Wall* advisory opinion, the ICJ considered "whether Israel could rely on a state of necessity, which would preclude the wrongfulness of the construction of the wall," but dismissed its applicability on the facts as it was not convinced that "the construction of the wall along the route chosen was the only means to safeguard the interest of Israel against the peril which it has invoked as justification for that construction."[61]

The plea of necessity is one among six circumstances identified by the ILC as precluding the wrongfulness of an otherwise unlawful act.[62] The ILC's decision to adopt a negative wording in defining the scope and content of necessity reveals its intention to underscore the exceptional nature of the plea. Article 25 of the Articles on State Responsibility states:

> 1. Necessity may not be invoked by a State as a ground for precluding the wrongfulness of an act not in conformity with an international obligation of that State unless the act:

---

59. While the majority of scholars have questioned the applicability of necessity as a plea involving uses of force, some have questioned the customary international law status of necessity as elaborated by the International Law Commission. *See*, *e.g.*, *id.*

60. Gabcikovo-Nagymaros Project (Hung./Slov.), 1997 I.C.J. 7, ¶ 51 (Sept. 25).

61. Wall Advisory Opinion, *supra* note 2, ¶ 140.

62. *See* CRAWFORD, *supra* note 18, at 160–89. The five other circumstances are consent (Article 20), self-defense (Article 21), countermeasures (Article 22), *force majeure* (Article 23) and distress (Article 24).

> (a) is the only way for the State to safeguard an essential interest against a grave and imminent peril; and
>
> (b) does not seriously impair an essential interest of the State or States towards which the obligation exists, or of the international community as a whole.
>
> 2. In any case, necessity may not be invoked by a State as a ground for precluding wrongfulness if:
>
> (a) the international obligation in question excludes the possibility of invoking necessity; or
>
> (b) the State has contributed to the situation of necessity.

The most compelling reason for preferring necessity over self-defense as a basis for justifying the use of force against a non-State actor is that, in contrast to self-defense, necessity is not dependent on a prior wrongdoing by the State acted against.[63] This aspect of the plea makes it particularly relevant in situations where there is little or no evidence to suggest that a State has been involved in an armed attack by a non-State actor. In contrast to Article 51, which leaves the victim State with no lawful option involving the use of defensive force, necessity would function to preclude responsibility for what would otherwise be a wrongful use of force by the victim State that is *totally independent* of the conduct adopted by the territorial State. In other words, necessity introduces the possibility of extending a lawful remedy to the victim State of an armed attack by a non-State actor without requiring it to attribute the wrongdoing to another State (including the ter-

63. The commentary to Article 33 on the State of Necessity to the ILC's 1980 report states, "[T]he wrongfulness of an act committed in a state of necessity is not precluded by the pre-existence . . . of a particular course of conduct by the State acted against." Rep of the Int'l Law Comm'n, 32nd sess, May 5–July 25, 1980, UN GAOR 35th Sess., Supp. No. 10, at 34, ¶ 2, U.N. Doc. A/35/10 (1980) [hereinafter 1980 Report of the ILC]. The commentary to the Draft Articles on State Responsibility likewise states, "Unlike consent (art. 20), self-defence (art. 21) or countermeasures (art. 22), [necessity] is not dependent on the prior conduct of the injured State." Draft Articles on Responsibility of States for Internationally Wrongful Acts, Rep. of the Int'l L. Comm'n, 53d Sess., U.N. GAOR 56th Sess., Supp. No. 10, at 178, ¶ 2, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 26, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2), *available at* http://untreaty.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf.

ritorial State from where the attack originates) in circumstances where there is clearly no such involvement on the part of a State in the attack. Since the victim State is likely to take the forcible measures it deems are necessary to defend its interests, it is simply a farce to leave it with no option but to present a case pursuant to Article 51 founded on contorted reasoning and dubious evidence linking the attack to the territorial State. By contrast, necessity would allow for a far more principled approach *governed by law* because a separation can be maintained between the wrongdoing perpetrated by the non-State actor and the relationship between the State deploying force and the territorial State in which such force is used.

For example, although Turkey did not expressly claim that its use of force in Iraq against the Kurdistan Workers' Party (PKK) in 1995 was justified by reason of necessity, its submissions to the Security Council justifying force were more redolent of necessity than self-defense in that Turkey made no effort to link its use of force to a prior wrongdoing on the part of Iraq. In fact the opposite was the case. During the course of its military operations against the PKK, which had established a number of bases within Iraq, Turkey emphasized that it had "always attributed utmost importance to the preservation of the sovereignty and territorial integrity of Iraq, a country with which it maintained close political and economic relations, emanating from a common historical background." Despite the mounting criticism and Libya's accusation that Turkey's incursion into Iraq was an act of aggression, it did not recall Article 51 as the United States had done on its behalf.[64] Instead, Turkey maintained that it could not "ask the Government of Iraq to fulfill its obligations, under international law, to prevent the use of its territory for the staging of terrorist acts against Turkey" since, due to the existing no-fly zone which had been imposed since 1991, Iraq was unable to exercise authority over the northern part of its country. Insofar as Turkey was concerned, it was "resorting to legitimate measures" against attacks by non-State actors to safeguard its own security which, in the particular circumstances, could not be regarded as a violation of Iraq's sovereignty.[65] Whether Turkey's military operations satisfied the requisite conditions of necessity is a wholly separate question that is discussed below.

---

64. Letter dated 12 July 1995 from the Charge d'Affaires A.I. of the Permanent Mission of the Libyan Arab Jamahiriya, U.N. SCOR, 50th Sess., U.N. Doc. S/1995/566 (July 12, 1995).

65. Letter dated 24 July 1995 from the Charge d'Affaires A.I. of the Permanent Mission of Turkey, U.N. SCOR, 50th Sess., U.N. Doc. S/1995/605 (July 24, 1995).

State practice in which the plea of necessity involving a use of force has been invoked is admittedly sparse. The leading pre-Charter case is the *Caroline* incident of 1837. Although frequently cited as an example of self-defense, close scrutiny of the exchanges between the UK and United States indicate that the case centered on the plea of necessity in a pre–*jus ad bellum* environment. For its part, the UK was adamant that its use of armed force on U.S. territory directed at non-State actors who were assisting the Canadian insurgents was lawful. The destruction of the *Caroline*, a vessel owned by American citizens which was being used to aid the Canadian insurgents, was, according to the British government, "a justifiable employment of force, for the purpose of defending the British Territory from the unprovoked attack of a band of British rebels and American pirates, who, having been 'permitted' to arm and organize themselves within the territory of the United States, had actually invaded a portion of the territory of Her Majesty."[66] From the exchanges that followed, it is clear that while the United States took offense with the inference that it had *allowed* the rebels to use its territory from which to launch such attacks, it was equally concerned to distance itself from the conduct of the rebels with the statement that it was the President's "fixed resolution that all such disturbers of the national peace, and violators of the laws of their country, shall be brought to exemplary punishment."[67]

The ILC's determination that the *Caroline* case turned on the principle of necessity rather than self-defense merits being cited in full:

> In response to the protests by the United States, the British Minister in Washington, Fox, referred to the "necessity of self-defence and self-preservation"; the same point was made by counsel consulted by the British Government, who stated that "the conduct of the British Authorities" was justified because it was "absolutely necessary as a measure of precaution". Secretary of State Webster replied to Minister Fox that "nothing less than a clear and absolute necessity can afford ground of justification" for the commission "of hostile acts within the territory of a Power at Peace", and observed that the British Government must prove that the action of its forces had really been caused by "a necessity of self-defence, instant, overwhelming, leaving no choice of means, and no moment for

66. Extract from note of April 24, 1841 from U.S. Secretary of State Daniel Webster to the British Government following an exchange with the British Minister in Washington, Mr. Fox, *available at* http://avalon.law.yale.edu/19th_century/br-1842d.asp (last visited Sept. 15, 2012).

67. *Id.*

> deliberation". In his message to Congress of 7 December 1841, President Tyler reiterated that:
>
> "This Government can never concede to any foreign Government the power, except in a case of the most urgent and extreme necessity, of invading its territory, either to arrest the persons or destroy the property of those who may have violated the municipal laws of such foreign Government."
>
> The incident was not closed until 1842, with an exchange of letters in which the two Governments agreed that "a strong overpowering necessity may arise when this great principle may and must be suspended". "It must be so", added Lord Ashburton, the British Government's ad hoc envoy to Washington, "for the shortest possible period during the continuance of an admitted overruling necessity, and strictly confined within the narrowest limits imposed by that necessity."[68]

Although the term "self-defence" appears in the exchanges between the parties, it is clear that each was referring to a state of necessity. What is more, the incident predated any limitation on the right of the use of force. Even though the *Caroline* case provides an exemplary example of necessity, the critical question is whether it is at all relevant in the post-Charter age.[69] Did the advent of the *jus ad bellum* regime with the express inclusion of Article 51 implicitly exclude necessity?

Before addressing these questions, the criticisms directed at the ILC for its apparent ambivalence as to whether necessity is a justification or excuse merits some comment.[70] To treat necessity as a justification is to suggest that the violation of the obligation owed by a State to another was, in the circumstances, not wrongful. If, on the other hand, necessity functions to excuse the State, no responsibility attaches for the violation although the act is recognized as wrongful. As commentators have observed, the difference between the two is of critical importance as legal consequences follow for victims (*Is compensation in order?*) and third parties (*Are they entitled to intervene?*). Although distinguishing between justifications and excuses within the context of domestic criminal law offers practical benefits and can inject

68. CRAWFORD, *supra* note 18, at 178, ¶ 5.

69. In his dissenting opinion in the *Corfu Channel* case, Judge Krylov concluded, "[T]he so-called right of self-help, also known as the law of necessity (Notrecht) which used to be upheld by a number of German authors, can no longer be invoked. [In the post-Charter age] it must be regarded as obsolete." Corfu Channel, *supra* note 27, at 77.

70. Sloane, *supra* note 58, at 483.

greater clarity into notions of culpability, whether the same reasoning applies at the international level is another matter.[71] The ILC's decision to retain the phrase "circumstances precluding wrongfulness" and, in parallel, remain agnostic as to whether any of the listed circumstances functioned to justify or excuse, might be better regarded as a recognition of the particular way in which international law is constituted. Exculpation may indeed weaken the compliance pull exercised by a rule to a greater extent than an excuse,[72] but there may be good reasons why on certain occasions a violation is regarded as justified. Since international law is an outcome of State practice, whether a circumstance serves to exculpate or excuse is a matter that is better treated on a case-by-case basis rather than through the imposition of "one blanket solution."[73] To transplant a legal methodology from the domestic to the international without due regard for the fundamentally distinguishable structural relations upon which each is founded is, as Robert Sloane observes, a "perilous" exercise.[74] Likewise, although the reasoning and conditions attached to the plea of necessity as it applies to States may be informed by the domestic experience, they should not be determined by it.

A. The Prohibition on the Use of Force in a Post-Charter System

To claim that the plea of necessity might be invoked to preclude responsibility for a use of force under contemporary international law is a controversial assertion. The predominant view is that the *jus ad bellum* regime introduced by the UN Charter prohibited all uses of force save for the two codified exceptions. What is more, even if the plea of necessity cannot preclude responsibility if the obligation violated is a peremptory norm. That the prohibition on the use of force as codified in Article 2(4) of the Charter is such a norm is widely accepted among international law experts.[75] Terry

71. Contrary to popular opinion, distinguishing between justifications and excuses within criminal law is often not easy. In particular, the difficulty associated with categorizing necessity and duress is such that they may better be approached as hybrid defenses.

72. Vaughan Lowe, *Precluding Wrongfulness or Responsibility: A Plea for Excuses*, 10 EUROPEAN JOURNAL OF INTERNATIONAL LAW 405, 410 (1999).

73. *Id.* at 411.

74. Sloane, *supra* note 58, at 473.

75. *See, e.g.*, CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 24 (2000); Bruno Simma, *NATO, the UN and the Use of Force: Legal Aspects*, 10 EUROPEAN JOURNAL OF INTERNATIONAL LAW 1, 2–3 (1999) (stating "the prohibition enunciated in Article 2(4) of the Charter is part of *jus cogens*, i.e., it is accepted and recognized by the in-

Gill's description of the prohibition as the "linchpin of the international legal system" is a commonly shared view, as is his observation that "although subjected to differing interpretations by scholars, and violated on numerous occasions, it nevertheless remains an almost universally accepted fundamental rule of international law and relations, one widely recognized as having a *jus cogens* character."[76] To question the *jus cogens* status of the prohibition comes close to undermining the entire edifice upon which contemporary international law is founded. That said, if the prohibition is indeed a peremptory norm, any views that hold otherwise should be easy to dismiss.

Overcoming these objections is admittedly difficult despite the rejection by the ILC and its Special Rapporteur, Robert Ago, of the suggestion that the express inclusion of the self-defense exception to the Article 2(4) prohibition in the Charter implicitly excluded the plea of necessity in all circumstances. Such a conclusion, it was maintained, did not "logically or necessarily" follow.[77] Whether such a finding is sustainable today is another matter. The record over the last sixty years is that States have consistently invoked self-defense to justify any and all uses of force even when the factual circumstances would have supported a strong claim of necessity, as in many cases involving the "rescuing" of nationals and others from civil war or hostage situations.

The objection—that the *jus cogens* status of the prohibition on the use of force that precludes the applicability of necessity—presents less of an impediment. Despite the consensus among a majority of commentators that the prohibition is *jus cogens*, on closer inspection there is surprisingly little evidence in the shape of explicit declarations on the part of States to

---

ternational community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same peremptory character"); ALEXANDER ORAKHELASHVILI, PEREMPTORY NORMS IN INTERNATIONAL LAW 50 (2006) ("the prohibition of the use of force by States *undoubtedly* forms part of *jus cogens*"). *See also* Separate Opinions of Judges Simma (¶¶ 329–30), Koojmans (¶ 260) and Elaraby (¶ 291) in *Oil Platforms*, *supra* note 28.

76. Terry D. Gill, *The Temporal Dimension of Self-Defence: Anticipation, Pre-emption, Prevention and Immediacy*, 11 JOURNAL OF CONFLICT AND SECURITY LAW 363 (2006).

77. Addendum to Eighth Report on State Responsibility by Mr. Roberto Ago, [1980] 2 YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 59, U.N. Doc. AICN.4/318/ ADD.5-7 [hereinafter Addendum to Eighth Report]. This question arose in the context of the agreement on the part of both the ILC and the Special Rapporteur that necessity could not preclude the wrongfulness of a primary obligation which, by its definition, excluded the possibility of invoking necessity. *See also* CRAWFORD, *supra* note 18, at 185, ¶¶ 19, 21.

support this view.[78] Of course this does not mean that the prohibition is not part of customary international law and therefore not binding on all States. The State practice in support of its customary status is considerable. Nevertheless, whether the prohibition as codified in Article 2(4) stands up to scrutiny when assessed against the generally accepted criteria for identifying a *jus cogens* norm demands consideration. This is a question that has received little attention given the significance of the outcome.[79] Article 53 of the 1969 Vienna Convention on the Law of Treaties defines a peremptory norm of general international law as "a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character." Since by definition, a *jus cogens* norm is generally accepted as one from which States may not derogate, the fact that the Article 2(4) prohibition is not an absolute rule but subject to a number of exceptions is problematic. The complexity of this issue is alluded to by former ICJ Judge Rosalyn Higgins, who comments:

> In the *Oil Platforms* case, some judges viewed the application of norms relating to the use of force as having this special [*jus cogens*] character, and for this reason among others, displacing the more obvious applicable law. It seems to me self-evident that the use of force, when it is prohibited in the circumstances of Article 2(4) of the Charter, but permitted in the circumstances of Article 51 of the Charter, is not a jus cogens provision that without more sets aside a different specific, applicable law.[80]

As Linderfalk reveals, the application of the definition of *jus cogens* to the prohibition appears to produce an absurd outcome: "[T]he relevant *jus cogens* norm cannot possibly be identical with the principle of non-use of force as such. If it were, this would imply that whenever a State exercises a right of self-defence, it would in fact be unlawfully derogating from a norm of *jus cogens*."[81] To surmount the critics' doubt as to the *jus cogens* status of

78. James Green, *Questioning the Peremptory Status of the Prohibition of the Use of Force*, 32 MICHIGAN JOURNAL OF INTERNATIONAL LAW 242, 254 (2011).

79. Addendum to Eighth Report, *supra* note 77, ¶ 59. The two notable exceptions are Ulf Linderfalk, *infra* note 81, and James Green, *supra* note 78.

80. Higgins, *supra* note 26, at 801.

81. Ulf Linderfalk, *The Effect of* Jus Cogens *Norms: Whoever Opened Pandora's Box, Did You Ever Think About the Consequences*?, 18 EUROPEAN JOURNAL OF INTERNATIONAL LAW 853, 860 (2007). Even those scholars who support the *jus cogens* status of the prohibition

the prohibition thus requires redefining the prohibition by incorporating the exceptions into the rule. What is more, a comprehensive remedy would also require the conditions imposed by customary international law to be similarly integrated into the definition.[82] The complexity of the challenge, coupled with the perpetually contested aspects of the right to use defensive force, has prompted some to question whether a *jus cogens* norm can exist when its scope and parameters for its application are so debated.[83]

A further factor that weakens the norm's *jus cogens* credentials is the uncertainty that surrounds the very notion of what constitutes a use of force. Although Article 2(4) prohibits the use of force, no further definition or criteria are provided under the Charter to determine when an act amounts to a use of force.[84] What is now widely accepted is that uses of force can be differentiated. This was expressly recognized by the ICJ in the *Nicaragua* judgment when it distinguished the uses of force that are "most grave"—those constituting an "armed attack"—from other, less grave forms of force.[85] Six years earlier, the ILC had raised this very question in the context of whether necessity could be invoked in situations involving uses of force that were not, by definition, in violation of a peremptory norm. Although there was unanimity that a use of force within the meaning of "aggression" would unambiguously violate a peremptory norm (thereby precluding the applicability of necessity) the more pertinent question was whether necessity could be invoked in situations that involved uses of force short of aggression if not all uses of force were peremptory in nature.[86]

A survey of State practice, at least until 1980, proved ambiguous, leading the ILC and its then–Special Rapporteur, Roberto Ago, to conclude that no definitive conclusions could be drawn. It therefore remained unset-

---

have conceded that "the peremptory rule banning the use of force does not exactly coincide with the corresponding rule contained in Art. 2(4) of the U.N. Charter." Natalino Ronzitti, *Use of Force,* Jus Cogens *and State Consent, in* THE CURRENT LEGAL REGULATION OF THE USE OF FORCE 147, 150 (Antonio Cassese ed., 1986).

82. Green, *supra* note 78, at 229–36.

83. *Id.* at 236.

84. TALLINN MANUAL, *supra* note 10, commentary to rule 11, ¶ 1.

85. Nicaragua Judgment, *supra* note 5, ¶ 191.

86. In the Addendum to the Eighth Report, Ago noted that "we were able to observe an outright rejection of the idea that a 'plea of necessity' could absolve a State of the wrongfulness attaching to an act of aggression committed by that State." Addendum to Eighth Report, *supra* note 77, ¶ 79. Similarly, "In the opinion of the Commission . . . no invocation of a 'state of necessity' can have the effect of precluding the international wrongfulness of conduct not in conformity with an obligation of *jus cogens*." 1980 Report of the ILC, *supra* note 63, at 43.

tled as to whether States were barred from invoking necessity in respect of all uses of force because, by definition, all are *jus cogens* prohibitions. This impasse of sorts was "resolved" by distinguishing between primary and secondary rules, allowing Ago to reason that since the ILC had been tasked to identify the applicable secondary rules, it was up to other organs charged with interpreting the primary rules to determine whether a differentiation could be made.[87] Finding Ago's reasoning persuasive, in its 1980 report the ILC also deferred judgment on the matter but nevertheless concurred with the Special Rapporteur's assessment that the question might arise as to whether a state of necessity could be invoked to justify an infringement of the territorial sovereignty of a State in circumstances where the violation need not necessarily be considered as an act of aggression or breach of a *jus cogens* obligation.[88]

According to the Commission, a distinction could be drawn for "certain actions by States in the territory of other States which, although they may sometimes be of a coercive nature, serve only limited intentions and purposes bearing no relation to the purposes characteristic of a true act of aggression."[89] More specifically, this could include:

> Some incursions into foreign territory to forestall harmful operations by an armed group which was preparing to attack the territory of the State, or in pursuit of an armed band or gang of criminals who had crossed the frontier and perhaps had their base in that foreign territory, or to protect the lives of nationals or other persons attacked or detained by hostile forces or groups not under the authority and control of the State, or to eliminate or neutralize a source of troubles which threatened to occur or to spread across the frontier.[90]

By 1999, the question of whether uses of force could be "differentiated" had become a particularly pressing matter in the context of the military action in Kosovo and the ensuing debates on humanitarian intervention. Endorsing his predecessor's reasoning, the newly appointed Special Rap-

87. Addendum to Eighth Report, *supra* note 77, ¶ 66. The Special Rapporteur did, however, note that to claim that all uses of force are prohibited *jus cogens* "might be to expand beyond what is at present accepted by the legal conviction of States, either the concept of 'aggression' or the concept of a 'peremptory norm' as defined in article 53 of the Vienna Convention on the Law of Treaties." *Id.,* ¶ 59.

88. 1980 Report of the ILC, *supra* note 63, at 43–44, ¶ 23.

89. *Id.* at 44.

90. *Id.*

porteur, James Crawford, concluded that the question of whether the use of force in certain circumstances was lawful was not a matter that fell within the scope of the secondary rules.[91] But despite the Special Rapporteur's repeated emphasis that it was *not* the function of the Commission to interpret the Charter provisions on the use of force, in his discussions on peremptory norms and humanitarian intervention, Crawford is clearly of the view that "the rules relating to the use of force referred to in Articles 2(4) and 51 of the Charter" rank among the "peremptory norms of international law."[92] The Special Rapporteur's insistence on maintaining a distinction between primary and secondary rules—thereby avoiding the fracas over humanitarian intervention—simply did not extend to the prohibition on the use of force as codified in Article 2(4) which was assumed to be a "peremptory norm."[93]

The final draft of the ILC's Articles on State Responsibility avoids all reference to the contentious question as to whether all uses of force are *jus cogens*. Nevertheless, fears that the inclusion of a list of circumstances that functioned to preclude wrongfulness would create a loophole led the Commission to include Article 26 ("Compliance with peremptory norms"). In that article, the Commission reaffirms that none of the listed circumstances can preclude the wrongfulness of an act which is not in conformity with an obligation arising under a peremptory norm. Conceding that few peremptory norms have been recognized by the international community as meeting the criteria set forth in Article 53 of the 1969 Vienna Convention, the Commission concludes that those peremptory norms that are clearly accepted include "the prohibitions of aggression, genocide, slavery, racial discrimination, crimes against humanity and torture, and the right to self-determination."[94] The absence of any reference to the prohibition on the use of force has left commentators to differ on what conclusions might be drawn.

While all uses of force are prohibited under treaty and customary international law, apart from the two codified exceptions, it is difficult to defini-

91. Crawford Second Report, *supra* note 57, ¶ 286. Over the years, the ILC continued to avoid the question on the grounds that it was not its function to interpret the Charter provisions on the use of force.

92. *Id*., ¶¶ 279, 286.

93. *Id*., ¶ 287.

94. CRAWFORD, *supra* note 18, at 188, ¶ 5. Article 26 states: "Nothing in this chapter precludes the wrongfulness of any act of a State which is not in conformity with an obligation arising under a peremptory norm of general international law."

tively conclude that all such prohibitions have acquired the status of a *jus cogens* prohibition.[95] However, even if a distinction in uses of force can be sustained, surmounting the argument that the plea of necessity involving a use of force did *not* survive the Charter regime remains hugely problematic. This raises the question as to whether necessity can or should be revived as an exception by virtue of a primary rule and, if so, what conditions might attach to best guard against abuse.

B. The Conditions Attached to the Doctrine of Necessity

Insofar as the acting State is concerned, invoking necessity implies perfect awareness of having deliberately chosen to act in a manner *not* in conformity with an international obligation.[96] Since the decision to violate the obligation must have been the "only way" to avert the threat, there is no room for a State wishing to rely on the plea to claim that the conduct chosen was the preferred option among other available options that would not have entailed a breach of the obligation. It is likely that most pleas based on necessity will be rejected at this stage. This particular condition of the necessity plea parallels the necessity requirement that attaches to self-defense in that it would be impermissible for the acting State to resort to force if other options to effectively address the threat are available. Take, for example, the incursions by Turkey into northern Iraq. There is an arguable case that since Iraq was unable to prevent the PKK from launching attacks from its territory given the existence of the no-fly zone, the *only way* that Turkey could avert further attacks was to take matters into its own hands which necessarily involved the violation of Iraq's territorial sovereignty. Whether Turkey's military operations fulfilled the remaining conditions of necessity so as to conclude that its responsibility for violating the obligation it owed to Iraq was precluded is another matter.

The use of the word "essential" by the ILC to denote what interests might be protected by the violation of an obligation has been criticized for

95. Few scholars are willing to question the *jus cogens* status of the prohibition on the use of force. *See, e.g.*, Ronzitti, *supra* note 82, at 153–54; Andreas Laursen, *The Use of Force and (the State of) Necessity*, 37 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 525 (2004).

96. *See* 1980 Report of the ILC, *supra* note 63, at 35 ("[T]he State organs which then have to decide on the conduct which the State will adopt are in no way in a situation that deprives them of their free will. It is certainly they who decide on the conduct to be adopted in the abnormal conditions of peril facing the State of which they are the organs, but their personal freedom of choice remains intact. The conduct adopted will therefore result from a considered, fully conscious and deliberate choice.").

being too broad in scope. The Commission's decision in 1980 that "it would be pointless to try to spell out any more clearly and to lay down pre-established categories of interests"[97] on the ground that such matters were invariably context-dependent was a view from which the ILC did not depart in the final draft. By way of example, in both 1980 and 2001, the ILC suggested that such interests might include preserving the existence of the State itself, its political or economic survival, the maintenance of conditions in which its essential services can function, the keeping of its internal peace, the survival of part of its population, and the ecological preservation of all or some of its territory.[98] Although these interests are admittedly broad in nature, it is only when the interest identified is threatened by a "grave and imminent" peril that the condition is satisfied. To return to the case of Turkey, unless compelling evidence of a grave and imminent attack by the PKK could have been demonstrated, it is unlikely that Turkey would have been able to rely on the plea. Other cases cannot be so easily dismissed, including Lebanon in 2006 and Afghanistan in 2001.

In addition to posing a serious threat to the interest identified, the peril must be "objectively established"; in other words, the *possibility* of a threat to the interest does not suffice. This does not mean that uncertainty as to the future disqualifies a State from invoking the plea but what *is* required is for the threat to be "clearly established on the basis of the evidence reasonably available at the time."[99] Moreover, the peril must be imminent in the sense of "proximate."[100] This raises an important question concerning temporality. As with self-defense, once the peril or threat no longer exists, there is no basis upon which the State can continue to rely on the plea. A State that resorts to force on the territory of another therefore cannot continue to invoke necessity once the threat no longer exists.

A further condition for invoking necessity is that the conduct in question must not seriously impair an essential interest of the other State or States concerned, or of the international community as a whole. This condition, as Sloane has observed, requires a balancing analysis that is akin to the choice-of-evils paradigm found in domestic criminal law. Sloane's concern that this assumes "values and interests can, in principle, be ranked ordinarily in a normative hierarchy" [101] is not, as he infers, one that is limited

97. *Id.* at 49, ¶ 32.
98. *Id.* at 35, ¶ 3. *See also* CRAWFORD, *supra* note 18, at 183, ¶ 14.
99. *See* CRAWFORD, *supra* note 18, at 184, ¶ 16.
100. *Id.*, ¶ 15.
101. Sloane, *supra* note 58, at 476.

to the arena of international law. At the municipal level the lesser harm test has never satisfactorily explained how an objective comparison can be made of harms that are plainly not quantifiable or where the values being compared are manifestly incommensurable because qualitatively so different. The lesser harm test is sometimes equated to the proportionality test although the former sets a higher threshold. The ILC decision to opt for the lesser-harm test therefore corresponds with its overall ambition to limit the applicability of the plea.

The fact that the interest relied on must "outweigh all other considerations, not merely from the point of view of the acting State but on a reasonable assessment of the competing interests, whether these are individual or collective," injects into the assessment a critical element of objectivity, including the requirement to consider obligations *erga omnes*.[102] This particular condition will severely curtail a State's ability to resort to force since the threat must be very substantial to outweigh all other considerations. The threat would certainly have to go beyond "acts of a sporadic character that cause occasional harm and inconvenience"[103] since the two rules being violated form the cornerstone of the international legal system—namely, the prohibition on the use of force and the principle of territorial sovereignty. For the threat to reach the required level of gravity, it is doubtful that a pattern of attacks will suffice. Although the ICJ has not entirely dismissed the "accumulation of events" theory in the context of self-defense, it is doubtful that the same reasoning can apply in the case of necessity.[104] This is because, as Andreas Laursen opines, to respond to a systemic threat with an exceptional ad hoc response is conceptually an "oxymoron."[105]

It is not uncommon in domestic criminal law for a defendant to be precluded from relying on the plea of necessity by what is sometimes referred to as the doctrine of prior fault. In other words a defendant cannot rely on necessity if he or she has contributed to the situation. At the municipal level, the doctrine serves two purposes: to restrict the availability of the plea and to reaffirm the centrality of moral choice above any expansive deterministic claims which would undermine the very substance of the criminal justice system. Article 25(2) of the Articles on State Responsibility precludes necessity if the State has "contributed to the situation of necessity." The purpose of this condition may be simply to limit even further the

102. Laursen, *supra* note 95, at 506.
103. SCHACHTER, *supra* note 3, at 170.
104. Nicaragua Judgment, *supra* note 5, ¶ 231.
105. Laursen, *supra* note 96, at 526.

availability of the necessity plea. Nevertheless, this particular condition sits uneasily within the broader understanding of necessity as a circumstance that precludes wrongfulness on the part of States.

This cursory review of the conditions that attach to necessity indicates that it is a plea with limited application. The stringent cumulative conditions that will need to be met are likely to severely restrict its applicability. Why then should any efforts be made to "resurrect" the plea?

V. CONCLUSION

As a matter of legal reasoning, and in contrast to self-defense, necessity offers a far more coherent basis upon which to justify the extraterritorial use of force against members of organized armed groups where the consent of the territorial State is not forthcoming. Although the stringent cumulative conditions that apply to the plea of necessity mean that it is likely to be available only under "certain very limited conditions,"[106] the anxiety that the plea engenders nevertheless remains entrenched. A partial explanation for this is that necessity poses two particular problems for liberal theory. First, because it has the potential to "validate decisions according to conscience or prejudice rather than according to law,"[107] necessity threatens liberalism's uncompromising fidelity to the rule of law. Second, by blurring the line between legislative, executive, and judicial responsibilities necessity seems to condone self-exemption which liberalism cannot tolerate. That said, the intuitive resistance to recognizing the plea in circumstances involving the use of force may be misplaced. Allowing for the plea in exceptional situations would extend to States an effective remedy which would be governed by, and judged according to, the legal criteria established by the plea. Critically, this would also provide an opportunity to reclaim the inter-State interpretation of Article 51 and make better sense of the ICJ's insistence that an armed attack within the meaning of the article is limited to situations in which there has been substantial involvement of a State.

The plea of necessity may enable a State, in very exceptional circumstances, to cross a border lawfully but the State will also be required to comply with other relevant bodies of law before its conduct is regarded as lawful. In some situations this will entail having to respect relevant human rights obligations, while other situations will be governed by the *jus in bello*.

---

106. CRAWFORD, *supra* note 18, at 183, ¶ 14.

107. John Parry, *The Virtue of Necessity: Reshaping Culpability of the Rule of Law*, 36 HOUSTON LAW REVIEW 407 (1999).

Circumstances that give rise to a plea of necessity will be exceedingly rare. The use of force on the territory of Afghanistan in respect of Al Qaeda in 2001 is perhaps one such case. Paradoxically, international law scholars who attempted to make sense of the law in the immediate wake of 9/11 showcased the *Caroline* case as a precedent for invoking self-defense against non-State actors. The *Caroline* case *was* the relevant precedent, on the basis not of self-defense, but rather of necessity. Over a decade on, there seems little point in revising history but that does not mean that lessons cannot be learned from past mistakes.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Networks in Non-International Armed Conflicts: Crossing Borders and Defining "Organized Armed Group"

Peter Margulies

89 INT'L L. STUD. 54 (2013)

Volume 89 2013

Networks in Non-International Armed Conflicts: Crossing Borders and Defining "Organized Armed Group"

*Peter Margulies**

I. INTRODUCTION

As Al Qaeda has dispersed, the precise definition of an "organized armed group" (OAG) under the law of armed conflict (LOAC) has become increasingly vital. The United States currently targets certain members of Al Qaeda and affiliated organizations not only in Afghanistan, but also in other countries.[1] However, while the elements of Al Qaeda that were present in Afghanistan immediately after September 11 presumably constituted an OAG, it is less clear that supposed affiliates outside Afghan-

* Professor of Law, Roger Williams University. I thank Laurie Blank, Geoff Corn and Rebecca Ingber for comments on a previous draft.

1. *See* John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism, Remarks at the Harvard Law School Program on Law and Security: Strengthening Our Security by Adhering to Our Values and Laws (Sept. 16, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an; *see also* Harold Hongju Koh, Legal Adviser, U.S. Department of State, Address at the Annual Meeting of the American Society of International Law: The Obama Administration and International Law (Mar. 25, 2010), *available at* http://www.state.gov/s/l/releases/remarks/139119.htm; *cf.* Robert M. Chesney, *Beyond the Battlefield, Beyond Al Qaeda: The Destabilizing Legal Architecture of Counterterrorism*, __ MICHIGAN LAW REVIEW (forthcoming 2013), *available at* http://ssrn.com/abstract=2138623, at 14–16 (discussing dilemmas in cross-border targeting decisions).

istan are part of the *same* OAG. The issue raises the stakes of targeting decisions. If affiliated groups are part of an OAG under the Al Qaeda "umbrella," then arguably the United States has the right to target them wherever they are.[2] But if groups outside Afghanistan are *not* part of Al Qaeda, then targeting them requires a separate armed conflict and a separate *jus ad bellum* justification for the use of force.[3] Formulating and applying the OAG criteria is therefore an essential enterprise.

This article responds to the high-stakes challenge with a pragmatic approach[4] along two axes. First, it argues for a broad interpretation of the definition of "organized armed group" framed by the International Criminal Tribunal for the former Yugoslavia (ICTY) in *Prosecutor v. Tadic*.[5] In practice, while the language of the definition appears to be narrow, case law and scholarship have often expanded the concept. Second, the article shows that terrorist groups generally, and Al Qaeda in particular, reveal a surprising degree of organization. Some of this organization takes unconventional forms, dictated by the special circumstances of terrorist networks. Yet terrorist groups actually have many of the same organizational needs as States, including the pervasive need to control agency costs. Moreover, Al Qaeda exists in a synergistic relationship with many regional groups, providing training and influencing their choice of targets. Strategic influence of this type is a sufficient justification for targeting affiliates.

This article proceeds in two parts. Part I outlines the lessons of case law and commentary regarding the definition of OAG. This part suggests

---

2. If the State in which the group is currently located is willing and able to deal with the threat, the United States should defer to that State's efforts. *See* Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VIRGINIA JOURNAL OF INTERNATIONAL LAW 483, 499–503 (2012) (exploring "unwilling or unable" test based on law of neutrality); *cf.* Karl S. Chang, *Enemy Status and Military Detention in the War Against Al-Qaeda*, 47 TEXAS INTERNATIONAL LAW JOURNAL 1, 25–36 (2011) (consulting neutrality law to define "enemy" who can be targeted or detained); Rebecca Ingber, *Untangling Belligerency from Neutrality in the Conflict with Al Qaeda*, 47 TEXAS INTERNATIONAL LAW JOURNAL 75 (2011) (cautioning that neutrality law does not provide useful guide for detention of non-State actors in non-international armed conflicts (NIACs)).

3. *See* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 204–11 (4th ed. 2005).

4. *See generally* MICHAEL J. GLENNON, THE FOG OF LAW: PRAGMATISM, SECURITY, AND INTERNATIONAL LAW 20 (2010) (recommending "broader and more flexible interpretive method").

5. *See* Prosecutor v. Tadic, Case No. IT-94-1-T, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 2, 1995).

that the language used may seem narrow, but has often been interpreted in a more flexible fashion. Part II discusses the status as OAGs of terrorist groups in general and Al Qaeda in particular. It concludes that such groups often possess the degree of organization required for recognition under the laws of armed conflict. Furthermore, Al Qaeda as a network often exercises strategic influence on its affiliates that justifies targeting.

II. ORGANIZING THE CASE LAW ON OAGS

Both case law and evolving trends on the ground have precipitated the problem of trans-regional conflicts and organized armed groups. State conflicts with organized non-State actors are considered conflicts not of an international character (NIACs).[6] At least at first blush, one would assume that a NIAC can take place only on the territory of a single State; if the territory of more than one State is involved, it seems incongruous to deny the "international character" of the conflict.[7] Moreover, treaties and case law have required that at least one party to an armed conflict be an OAG. Additional Protocol II (AP II) defines OAG in a narrow way. According to AP II, OAGs must be "under responsible command, [and] exercise such control over a part of [a State's] territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol."[8]

---

6. *See* Hamdan v. Rumsfeld, 548 U.S. 557, 628–32 (2006).

7. *See* INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS 10 (2011), *available at* http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-LOAC-challenges-report-11-5-1-2-en.pdf [he reinafter IHL CHALLENGES] (discussing "multinational NIACs [in which] . . . multinational armed forces are fighting alongside the armed forces of a 'host' state—in its territory—against one or more organized armed groups" as well as "transnational" conflict between "Al Qaeda and its 'affiliates' and 'adherents' and the United States"); *see generally* Kenneth Watkin, *"Small Wars": The Legal Challenges*, *in* NON-INTERNATIONAL ARMED CONFLICT IN THE TWENTY-FIRST CENTURY 3 (Kenneth Watkin & Andrew J. Norris eds., 2012) (Vol. 88, U.S. Naval War College International Law Studies) (discussing dilemmas in conflicts against non-State actors); *cf.* Geoffrey Corn & Eric Talbot Jensen, *Transnational Armed Conflict: A "Principled" Approach to the Regulation of Counter-Terror Combat Operations*, 42 ISRAEL LAW REVIEW 1, 10–12 (2009) (arguing that NIAC concept does not fit well in analyzing conflicts involving global terrorist network such as Al Qaeda and suggesting "transnational armed conflict" as a superior alternative).

8. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, art. 1(1), June 8, 1977, 1125 U.N.T.S. 609.

Some groups, like Hamas in Gaza or the now-defunct Liberation Tigers of Tamil Eelam (LTTE) of Sri Lanka, might meet this definition, but a network such as Al Qaeda will not. Al Qaeda's dispersion therefore makes precise definition a priority.

A. The High Stakes of LOAC Definitions

Much hinges on the breadth of the definition of a NIAC. A narrow definition subjects State forces to the more rigorous demands of international human rights law (IHRL), which permits the use of deadly force only when an individual poses a concrete, imminent threat to the life of a law enforcement officer or other individuals.[9] The European Court of Human Rights has defined such threats narrowly, second-guessing the use of lethal force by law enforcement even when the target was a pair of known terrorists whom authorities rightly believed had planted an explosive device to be triggered in the near future.[10] Under IHRL, terrorists have a greater opportunity to operate with impunity. Applying LOAC, in contrast, diminishes the non-State actor's room to maneuver. It allows States to target individuals whom it believes to be performing a continuous combat function (CCF).[11] Even narrow definitions of CCF recognize that an individual who

9. *See* McCann v. United Kingdom, App. No. 18984/91, 21 Eur. H.R. Rep. 97 (1995); Geoffrey S. Corn, *Extraterritorial Law Enforcement or Transnational Counterterrorist Operations: The Stakes of Two Models*, *in* NEW BATTLEFIELDS, OLD LAWS: CRITICAL DEBATES ON ASYMMETRIC WARFARE 23, 35 (William C. Banks ed., 2011) (analyzing the relationship between LOAC and law enforcement paradigms); John B. Bellinger III & Vijay M. Padmanabhan, *Detention Operations in Contemporary Conflicts: Four Challenges for the Geneva Conventions and Other Existing Law*, 105 AMERICAN JOURNAL OF INTERNATIONAL LAW 201, 210–13 (2011) (same); *see also* Evan J. Criddle, *Proportionality in Counterinsurgency: A Relational Theory*, 87 NOTRE DAME LAW REVIEW 1073 (2012) (arguing that IHRL paradigm fits most cases involving violence by a State's nationals within a State's own territory); David Luban, *Military Lawyering and the Two Cultures Problem*, 25 LEIDEN JOURNAL OF INTERNATIONAL LAW __ (forthcoming 2013), *available at* http://ssrn.com/abstract=2054832 (asserting that law of armed conflict shows insufficient regard for welfare of civilians and that human rights law is superior in this respect); *cf.* Monica Hakimi, *A Functional Approach to Targeting and Detention*, 110 MICHIGAN LAW REVIEW 1365 (2012) (arguing for functional criteria that transcend distinction between LOAC and IHRL).

10. *See McCann*, App. No. 18984/91 ¶¶ 7–22 (Ryssdal, J., dissenting); *cf.* Peter Margulies, *Valor's Vices: Against a State Duty to Risk Forces in Armed Conflict*, *in* SHAPING A GLOBAL LEGAL FRAMEWORK FOR COUNTERINSURGENCY: NEW DIRECTIONS IN ASYMMETRIC WARFARE 87, 99 (William C. Banks ed., Oxford Univ. Press, 2013) (critiquing *McCann*).

11. *See* HCJ 769/02 The Public Committee Against Torture in Israel v. The Government of Israel, ¶ 39 [2006] (Isr.), http://elyon1.court.gov.il/files_eng/02/690/007

performs this role may spend much time in pursuits other than presenting a concrete, imminent threat to the other side. A typical uniformed soldier, for example, may spend time marching, building an encampment or even sleeping. The soldier can be targeted by an enemy State's forces in any and all of these activities.[12] Just as a State can target an opposing State's uniformed forces without a showing that an individual soldier faces a specific, imminent threat, LOAC would allow targeting of a member of an armed group whom the State reasonably believed to be engaged in a CCF.

However, the greater latitude allowed States in targeting terrorists makes human rights advocates blanch at the prospect of higher civilian casualties.[13] More latitude in targeting may increase the risk of mistakes, in

/A34/02007690.a34.pdf%20 (asserting that fighters who makes themselves regularly available to terrorist groups for acts of violence are directly participating in hostilities for such time as they make themselves available; any interlude between acts of violence is merely "preparation" for further violence). In this analysis, the *PCAT* Court lent a flexible reading to concepts that the International Committee of the Red Cross (ICRC) has defined more narrowly. *See* NILS MELZER, INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 54 (2009), *available at* http://www.aco.nato.int/resources/20/Legal%20Conference/ICRC_002_0990.pdf (arguing that terrorist bomb maker would be immune from targeting when not making bombs); *see also* Gabor Rona, *US Targeted Killing Policy Unjustified*, JURIST (Feb. 24, 2012), http://jurist.org/hotline /2012/02/gabor-rona-targeted-killing.php (criticizing United States' targeting standards as unduly broad); *but see* Michael N. Schmitt, *Deconstructing Direct Participation in Hostilities: The Constitutive Elements*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW & POLITICS 697, 731 (2010) (criticizing narrow reading in ICRC *Guidance*); Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW & POLITICS 641, 661 (2010) (criticizing ICRC's failure to dismantle "revolving door" mechanism for terrorist groups).

12. *See* MICHAEL WALZER, JUST AND UNJUST WARS: A MORAL ARGUMENT WITH HISTORICAL ILLUSTRATIONS 143 (1977); *but see* Gabriella Blum, *The Dispensable Lives of Soldiers*, 2 JOURNAL OF LEGAL ANALYSIS 115, 138–50 (2010) (questioning whether use of lethal force should always be permissible against uniformed combatants).

13. *See* Jens David Ohlin, *The Duty to Capture*, 97 MINNESOTA LAW REVIEW (forthcoming), *available at* http://ssrn.com/abstract=2131720. Although the definition of an OAG is relevant to targeting decisions, the targeting debate also raises other issues beyond the scope of this article. *Compare* Kenneth Anderson, *Efficiency* In Bello *and* Ad Bellum*: Making the Use of Force Too Easy?*, *in* TARGETED KILLINGS: LAW AND MORALITY IN AN ASYMMETRICAL WORLD 374, 391–96 (Claire Finkelstein, Jens David Ohlin & Andrew Altman eds., 2012) (rejecting argument that sophisticated technology behind drones that makes targeted killing easier also undermines practical checks on willingness to wage war); Robert M. Chesney, *Who May Be Killed? Anwar Al-Awlaki as a Case Study in the International Legal Regulation of Lethal Force*, 13 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 3

which a State erroneously targets innocents or causes collateral damage among civilians.[14] Advocates of greater State latitude will argue that States can and should build in systems that minimize mistakes, such as a lawyer's review and approval of targeting decisions. However, State advocates would add, opponents of State latitude have a bad case of hindsight bias[15] regarding State action. State critics regard all civilian casualties as avoidable, a position that the law of war has never taken. However, proponents of State latitude would argue, critics fail to consider matters from an *ex ante* perspective, involving the incentives for violent non-State actors. When violent non-State actors believe they can operate with impunity, risks to civilians increase.[16] Curbing violent non-State actors thus reduces net risks for civilians.

(2011) (suggesting that targeted killing under certain conditions is consistent with LOAC); Peter Margulies, *The Fog of War Reform: Change and Structure in the Law of Armed Conflict After September 11*, 95 MARQUETTE LAW REVIEW 1417, 1471–77 (2012) (same); Jordan J. Paust, *Self-Defense Targetings of Non-State Actors and Permissibility of U.S. Use of Drones in Pakistan*, 19 JOURNAL OF TRANSNATIONAL LAW & POLICY 237 (2010) (asserting that targeted killing is legal under international law as long as targeting force observes principles of distinction and proportionality), *with* PHILIP ALSTON, HUMAN RIGHTS COUNCIL, REPORT OF THE SPECIAL RAPPORTEUR ON EXTRAJUDICIAL, SUMMARY OR ARBITRARY EXECUTIONS (2010) (arguing that targeted killing in State that is not geographic site of armed conflict violates international law); Mary Ellen O'Connell, *Unlawful Killing with Combat Drones: A Case Study of Pakistan, 2004–2009*, *in* SHOOTING TO KILL: THE LAW GOVERNING LETHAL FORCE IN CONTEXT (Simon Bronitt ed., 2011); *cf.* Jennifer C. Daskal, *The Geography of the Battlefield: A Framework for Detention and Targeting Outside the "Hot" Conflict Zone*, 161 UNIVERSITY OF PENNSYLVANIA LAW REVIEW __ (forthcoming 2013), *available at* http://ssrn.com/abstract=2049532 (suggesting additional guidelines to regulate targeted killings).

14. *But see* JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11, at 131 (2012) (noting involvement of military lawyers in targeting decisions as check on errors); Gregory McNeal, *Are Targeted Killings Unlawful: A Case Study in Empirical Claims Without Empirical Evidence*, *in* TARGETED KILLINGS, *supra* note 13, at 326, 331–42 (discussing process engaged in by U.S. military prior to authorization of drone strike).

15. *See* Neal J. Roese, *Twisted Pair: Counterfactual Thinking and the Hindsight Bias*, *in* BLACKWELL HANDBOOK OF JUDGMENT AND DECISION MAKING 258, 260–61 (Derek J. Koehler & Nigel Harvey eds., 2004) (describing hindsight bias as "tendency to believe that an event was predictable before it occurred, even though for the perceiver it was not" and that harm was avoidable even when it was impossible to prevent).

16. *See* Margulies, *supra* note 10; Michael W. Lewis, *Drones and the Boundaries of the Battlefield*, 47 TEXAS INTERNATIONAL LAW JOURNAL 293 (2012) (suggesting that narrow geographic restrictions on States' ability to target terrorist groups with global operations would grant these groups asymmetric advantage).

Moreover, State critics often do not acknowledge that while a broader definition of OAG confers advantages on a State in the arena of targeting, with that advantage comes greater accountability for all parties to the NIAC.[17] A State in a NIAC must observe the strictures of the Geneva Conventions' Common Article 3, such as humane treatment of captives.[18] These provisions are generally considered *jus cogens* and therefore non–derogable.[19] OAGs incur the same duties; one purpose of the requirement that a group have a minimum level of organization is that it would be unfair to require a disorganized group to observe LOAC without possessing the structure to do so. Individuals who target civilians can be made to answer for violations of municipal law, such as the prohibition on murder. In contrast, OAGs who target civilians may be prosecuted in international tribunals for crimes against humanity, instead of merely being answerable in the sometimes dysfunctional justice systems of their countries of origin. The targeting advantages reaped by States are thus paid for by greater accountability elsewhere in the LOAC framework.[20]

B. Unpacking the ICTY Formulation

At first blush, State critics may have an edge in the definitional debate regarding OAG. Some passages in case law have propounded a narrow definition of OAG that requires something approaching the attributes of States.[21] In *Prosecutor v. Limaj*, the ICTY suggested that to meet its criteria, an OAG should have a headquarters, a unified command and a military

17. *See* Ohlin, *supra* note 13, at 21–22.

18. *See* Convention Relative to the Protection of Civilian Persons in Time of War, art. 3, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

19. IHRL provisions are often subject to derogation. *Cf.* IHL CHALLENGES, *supra* note 7, at 15 (describing applicability and scope of IHRL, particularly extraterritorial applicability, as "work in progress").

20. *See* United Nations Human Rights Council, Report of the Independent International Commission of Inquiry on the Syrian Arab Republic, U.N. DOC. A/HRC/21/50, ¶ 134 (Aug. 16, 2012), *available at* http://reliefweb.int/sites/reliefweb.int/files/resources/A-HRC-21-50_en.pdf (noting accountability under LOAC of anti-government armed groups in Syria) [hereinafter U.N.H.C.R., *Independent International Commission Report*].

21. *See* Prosecutor v. Limaj, Case No. IT-03-66-T, Trial Chamber Judgment, ¶¶ 113–117 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 30, 2005) [hereinafter Limaj]; *cf.* Jelena Pejic, *The Protective Scope of Common Article 3: More than Meets the Eye*, 93(881) INTERNATIONAL REVIEW OF THE RED CROSS 189, 191–92 (2011) (noting factors).

police unit that will arrest malefactors.[22] Without these attributes, a group is considered to be a criminal band or an assemblage of individuals engaged in civil unrest such as a riot, rather than an OAG.[23] Individuals in such groups cannot be targeted as readily as participants in an armed conflict, but instead are protected by IHRL.

Acts of terrorism sit uneasily within this paradigm. "[I]solated acts of terrorism" probably do not demonstrate the level of organization required for a NIAC.[24] Moreover, some commentators have noted that several major nations have addressed significant acts of terrorism through traditional law enforcement means.[25]

If a terrorist entity can elude definition as an OAG within one State, it can even more readily elude such definition in the regional or global context. The United States confronts extremist organizations with varying degrees of closeness to Al Qaeda in multiple regions. Some have argued that Al Qaeda's relationship to such groups involves only "very loose ties" typical of a "confederation of like-minded fellow travelers, many of whom are fighting *separate* armed conflicts in different regions of the globe."[26]

---

22. Limaj, *supra* note 21, ¶ 113–17; *see also* Prosecutor v. Akayesu, Case No. ICTR-96-4-T, Trial Chamber Judgment, ¶ 626 (Int'l Crim. Trib. for Rwanda Sept. 2, 1998) ("responsible command" entails "degree of organization [that permits the group] . . . to plan and carry out concerted military operations, and to impose discipline"; group must also "dominate a sufficient part of territory" and "operations must be continuous and planned").

23. In some cases, a criminal enterprise may be so organized and its violence against State officials so intense that classification as a NIAC is appropriate. *See* Carina Bergal, Note, *The Mexican Drug War: The Case for a Non-International Armed Conflict Classification*, 34 FORDHAM INTERNATIONAL LAW JOURNAL 1042 (2011).

24. *See* Prosecutor v. Boskoski & Tarculovski, Case No. IT-04-82-T, Trial Chamber Judgment, ¶ 190 (Int'l Crim. Trib. for the Former Yugoslavia July 10, 2008) [hereinafter *Boskoski*].

25. *See* INTERNATIONAL LAW ASSOCIATION, FINAL REPORT ON THE MEANING OF ARMED CONFLICT IN INTERNATIONAL LAW 25 (2010); *cf.* Kim Lane Scheppele, *The International Standardization of National Security Law*, 4 JOURNAL OF NATIONAL SECURITY LAW & POLICY 437, 451 (2010) (asserting that global counterterrorism measures permit States to disguise substandard governance as counterterrorism); Sudha Setty, *Comparative Perspectives on Specialized Trials for Terrorism*, 63 MAINE LAW REVIEW 131, 153 (2010) (suggesting that counterterrorism policies in United States, United Kingdom and India raise human rights concerns).

26. *See* Jens David Ohlin, *Targeting Co-Belligerents*, *in* TARGETED KILLINGS, *supra* note 13, at 60, 75 (emphasis added) (noting this view while not necessarily endorsing it); Craig Martin, *Going Medieval: Targeted Killing, Self-Defense and the* Jus ad Bellum *Regime*, *in* TARGETED KILLINGS, *supra* note 13, at 223, 245–46 (suggesting that groups with nominal Al

Treaty law and the ICTY jurisprudence actually permit greater flexibility in the definition of OAGs. While AP II applies to some NIACs, other NIACs are governed by Common Article 3, which contains no requirement that a party control territory.[27] The International Committee of the Red Cross (ICRC), a group with special competence regarding LOAC, has also signaled that flexibility is important. In one study, the ICRC observed that to be considered an OAG, an entity should merely have a "minimum of organization."[28] That terminology strongly suggests that a rigid, itemized checklist would be counterproductive.[29]

Moreover, the ICTY jurisprudence is far more flexible than it may appear.[30] In *Prosecutor v. Boskoski & Tarculovski*,[31] a case involving the targeting of civilians by a non-State group, the ICTY noted that terrorist acts could form a pattern that would constitute an armed conflict.[32] *Boskoski* can be read as standing for either one or two eminently pragmatic propositions.

Qaeda ties actually have little in common); *see also* Robin Geiß, *Armed Violence in Fragile States: Low-Intensity Conflicts, Spillover Conflicts, and Sporadic Law Enforcement Operations by Third Parties*, 91(873) INTERNATIONAL REVIEW OF THE RED CROSS 127, 134–35 (March 2009) (global Al Qaeda network structure appears "rather basic" and "rudimentarily organized"); *cf.* Ohlin, *supra* note 13 (offering more pragmatic view).

27. Ohlin, *supra* note 13, at 11–12; Michael N. Schmitt, *Unmanned Combat Aircraft Systems and International Humanitarian Law: Simplifying the Oft Benighted Debate*, 30 BOSTON UNIVERSITY INTERNATIONAL LAW JOURNAL 595, 604–06 (2012) (discussing relationship between AP II and Common Article 3); *cf.* Andreas Paulus & Mindia Vashakmadze, *Asymmetrical War and the Notion of Armed Conflict – A Tentative Conceptualization*, 91(873) INTERNATIONAL REVIEW OF THE RED CROSS 95, 117 (Mar. 2009) (discussing importance of flexibility in definition of an OAG).

28. *See* INTERNATIONAL COMMITTEE OF THE RED CROSS, HOW IS THE TERM "ARMED CONFLICT" DEFINED IN INTERNATIONAL HUMANITARIAN LAW? 5 (2008), http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf.

29. However, the ICRC has also indicated that the criteria mentioned in the ICTY jurisprudence are useful guides. *See* IHL CHALLENGES, *supra* note 7, at 8 (requiring a "certain level of organization," which may include, but is not limited to, "the existence of a command structure . . . disciplinary rules . . . headquarters," and logistical, attack, and negotiating capabilities).

30. *See* Ohlin, *supra* note 13, at 14 ("legal support for [requiring] centralization is misplaced"); Michael N. Schmitt, *The Status of Opposition Fighters in a Non-International Armed Conflict*, *in* Non-International Armed Conflict in the Twenty-First Century 119, 129 (Kenneth Watkin & Andrew Norris eds., 2012) (Vol. 88, U.S. Naval War College International Law Studies) (arguing that group's structure "need not be strictly hierarchical or implemented in any formalistic manner").

31. *Boskoski*, *supra* note 24.

32. *Id.* ¶ 185 (noting that terrorism may be part of NIAC if it is part of "protracted campaign").

First, OAGs should not be assessed in a vacuum, but on a sliding scale that also includes the other *Tadic* criterion, intensity.[33] Second, the best proof of an OAG is in the operational details of the violence that members of the group have caused. A group's sheer ability to mount sustained terrorist attacks is evidence of a "high level of planning and a coordinated command structure."[34]

The ICTY's finding that evidence of discipline exists also suggests substantial flexibility in the definition of an OAG. In *Limaj*, for example, the ICTY found that the Kosovo Liberation Army (KLA) was organized even though evidence of discipline was "scant" by the court's own admission.[35] Witnesses differed widely on when the military police cited by the tribunal had been established.[36] If the military police were a salient symbol of organizational discipline, this divergence in recollection seems odd. Moreover, as the ICTY acknowledged, there was no record of any imposition of discipline among KLA members.[37]

The *Limaj* court sought to buttress this decidedly equivocal evidence of discipline with a proxy: other nations and entities dealt with the KLA in a way that suggested that they regarded the group as organized,[38] although evidence for this point was slim. For example, the ICTY acknowledged that representatives of States and other entities were "sometimes unclear about the KLA's command structure."[39] Indeed, one report described the KLA's structure as "a mystery" and "more a matter of diffuse horizontal command."[40] *Limaj* also noted that the General Staff of the KLA "did not have a consistent . . . location."[41] The Tribunal acknowledged that the authorship and date of the KLA's governing regulations were not apparent

33. *Id.* ¶¶ 182–83; *see also* Laurie R. Blank & Geoffrey S. Corn, *Losing the Forest for the Trees: Syria, Law, and the Pragmatics of Conflict Recognition*, 46 VANDERBILT JOURNAL OF TRANSNATIONAL LAW __ (forthcoming 2013), *available at* http://ssrn.com/abstract=2029989, at 22–23 (discussing flexibility in ICTY approach); U.N.H.C.R., *Independent International Commission Report*, *supra* note 20, ¶ 134 (asserting that anti-government armed groups in Syria should be considered OAGs that are accountable under LOAC).

34. *Boskoski*, *supra* note 24, ¶ 204.

35. Limaj, *supra* note 21, ¶ 116.

36. *Id.* ¶ 113.

37. *Id.* ¶ 116.

38. *See* Limaj, *supra* note 21, ¶¶ 128–29.

39. *Id.* ¶ 131 (citing Austrian Embassy report).

40. *Id.* ¶ 131 (also observing that American diplomat Richard Holbrooke seconded this perception).

41. *Id.* ¶ 104.

on the regulations' face.[42] Yet the ICTY brushed past these apparent failures of organization, explaining pragmatically that the KLA was "effectively an underground operation, operating in conditions of secrecy out of concern to preserve its leadership" and "under constant threat of military action" by Serbian forces.[43] Therefore, it was "no surprise that the organizational structure and the hierarchy of the KLA was confusing."[44] More than any other factor, the court relied on the KLA's knack for recruiting new followers.[45] On the basis of this one criterion and modest evidence of others, the court was satisfied that the KLA's fluid and contingent structure did not undermine its classification as an OAG.

Precedent from elsewhere also argues against a narrow definition of organization. Consider *Abella v. Argentina (Tablada Case)*,[46] involving an attack on an Argentinean army base by rebels, followed by alleged State mistreatment of the attackers that the plaintiffs characterized as a violation of Common Article 3. The Inter-American Commission on Human Rights (IACHR) first ruled that AP II did not limit the situations in which armed conflict existed. The tribunal observed that armed conflicts "not of an international character" that trigger Common Article 3 need not be "large-scale and generalized hostilities or a situation comparable to a civil war in which dissident armed groups exercise control over parts of national territory."[47] Suggesting the need for flexibility, the IACHR noted that NIACs could also involve "confrontations between *relatively* organized armed forces."[48] The tribunal's use of the term "relatively" to modify the requirement of an OAG suggests that a narrow or rigid definition would be counterproductive. While the tribunal added that an armed conflict must be something more than "riots, mere acts of banditry or an unorganized and short-lived rebellion,"[49] its analysis indicated that requiring a significantly more elaborate showing would merely allow parties to escape accountability.

---

42. *Id.* ¶ 110; *see also id.* ¶ 124 (discussing KLA's lack of communications equipment).

43. *Id.* ¶ 132; *cf.* Daniel Byman & Matthew C. Waxman, *Kosovo and the Great Air Power Debate*, INTERNATIONAL SECURITY, Spring 2000, at 25 (finding that KLA failed to show "that it was capable of holding territory against the Serbian Army"); *id.* at 28 (describing KLA as initially "poorly organized" and as gaining strength only with NATO assistance).

44. Limaj, *supra* note 21, ¶ 132.

45. *Id.* ¶ 118.

46. Juan Carlos Abella v. Argentina, Case 11.137, Inter-American Commission on Human Rights, Report No. 55/97, ¶ 152 (Nov. 18, 1997) [hereinafter *Tablada Case*].

47. *Id.* ¶ 152.

48. *Id.* (emphasis added).

49. *Id.*

Turning to the specific facts, the IACHR found it sufficient that the rebels' attack on the base was "carefully planned, coordinated and executed."[50]

Tribunals have also expansively defined a non-State actor's capacity to comply with LOAC. Terrorist groups generally do not comply with LOAC; often their standard operating procedure involves fundamental violations such as the targeting of civilians. But tribunals have viewed terrorist groups as *able* to comply with LOAC, even if those groups are disinclined to do so.[51] A contrary view would create perverse incentives, allowing a group to free itself from the risk of targeting by increasing its violations of otherwise applicable norms.[52]

Buttressing this flexible approach, the ICTY has also broadly interpreted the *Tadic* requirement that violence be "protracted." Interpreting the term "protracted" narrowly would again create perverse incentives. Violent non-State actors could strike first and then claim that the conflict was not yet a protracted one, thereby precluding a State from utilizing the full range of responses permissible under LOAC. Instead, the State would be limited to the far narrower repertoire of force permissible under a law enforcement paradigm. To avoid creating this perverse incentive, the ICTY has viewed the term "protracted armed violence" in a pragmatic fashion, as referring generally to the intensity of the violence, not its timing per se.[53]

III. MORE THAN MEETS THE EYE: THE ORGANIZATION OF TERRORIST NETWORKS

Just as a deeper look at case law suggests that the definition of OAG is more flexible than it initially appears, terrorist groups are more organized

50. *Id.* ¶ 155. While the International Criminal Tribunal for Rwanda set out a narrower standard in *Prosecutor v. Akayesu*, that standard has generally not been followed and "is regarded as exceedingly high." *See* Geiß, *supra* note 26, at 136 n.40.

51. *See Boskoski*, *supra* note 24, ¶¶ 204–5 (pattern of LOAC violations does not support inference that group is unable to comply).

52. *Cf. id.* at 205 (explaining that tribunal "cannot merely infer a lack of organization . . . [because] international humanitarian law was frequently violated by [the group's] members").

53. *See* Prosecutor v. Haradinaj, Case No. IT-04-84-T, Trial Chamber Judgment, ¶ 49 (Int'l Crim. Trib. for the Former Yugoslavia Apr. 3, 2008) (noting the term "protracted armed violence" has been "interpreted in practice… as referring more to the intensity of the armed violence than to its duration"); *see also Tablada Case*, *supra* not 46, ¶ 156 (noting that "brief duration" of attack did not preclude classification as NIAC); *cf.* Paulus & Vashakmadze, *supra* note 27, at 106–07 (arguing that *Tadic* "protracted armed violence" criterion refers to intensity as well as duration).

than their historical image suggests. Although some scholars have viewed earlier acts of terror as the product of individual discontent, they actually involved careful planning.[54] Today's terrorist groups, including Al Qaeda, also display far more organization than is commonly understood.

A. Terrorist Groups, Organization and Agency Costs

Terrorist groups require organization because they wish to influence actors who are often organized. Terrorist groups play a multi-level game of the kind made famous by Robert Putnam, involving internal and external actors.[55] Internal actors include people within the organization and within the community that the group purports to represent—Al Qaeda claims to stand for a particular religious vision, while a group like Hamas purports to represent Palestinians and the Kurdistan Workers' Party (PKK) Kurds. External actors include States where the terrorist group is principally located, other States where the group wishes to extend its influence, groups of States such as Western nations or States in the Middle East, international organizations, and other terrorist groups.[56]

Terrorist groups use violence for both expressive and instrumental ends. Violence expresses their commitment to a distinctive vision that the mundane corruption of other parties obscures.[57] Certain kinds of violence, such as suicide attacks, communicate this commitment in an even clearer form—sending a message about the group's dedication to its cause.[58] Instrumentally, violence serves as a spoiler, derailing negotiations between States and moderate members of the group's own community.[59] On occasion, terrorist groups find it expedient to mitigate violence, to avoid alienat-

54. *See* Bruce Hoffman, *The Myth of Grass Roots Terrorism* (Book Review), 87(3) FOREIGN AFFAIRS 133, 135–36 (2008) (discussing careful organization behind assassination of Austrian Archduke Franz Ferdinand, which precipitated World War I).

55. *See* Robert D. Putnam, *Diplomacy and Domestic Politics: The Logic of Two-Level Games*, 42 INTERNATIONAL ORGANIZATION 427 (1988).

56. *See* Max Abrahms, *What Terrorists Really Want: Terrorist Motives and Counterterrorism Strategy*, INTERNATIONAL SECURITY, Spring 2008, at 85–86; Erica Chenoweth et al., *What Makes Terrorists Tick?*, INTERNATIONAL SECURITY, Spring 2009, at 83.

57. *See* BRUCE HOFFMAN, INSIDE TERRORISM 168–69 (1998).

58. *See* Abrahms, *supra* note 56, at 85–86.

59. *Cf.* Andrew H. Kydd & Barbara F. Walter, *The Strategies of Terrorism*, INTERNATIONAL SECURITY, Summer 2006, at 72–75 (explaining incentives for violent extremists to undermine peace negotiations).

ing key constituencies or to gain time to regroup from State pressure.[60] Managing violence to maximize both expressive and instrumental goals requires organization. Maintaining fidelity to these goals in the face of State pressure and internal disagreement requires a particular agility in organizational form.

Like any other entity, a terrorist group needs some form of discipline. Without discipline, agency costs proliferate, as undisciplined members pursue their own impulses or agendas to the detriment of the organization's goals.[61] However, discipline requires institutional memory, as leaders monitor, document and assess the performance of subordinates. Documentation can be exploited by the group's foes, providing information about operatives and planned attacks. Terrorist groups, including Al Qaeda, grapple with the conflict between uniform messaging and secrecy.

Al Qaeda has coped with this dilemma by cultivating a portfolio approach that maximizes versatility in structure and decision making, as well as in operational plans.[62] Wise investors use portfolio theory to diversify risk. The careful and prudent investor never entrusts all of her resources to one company or even one sector. Rather, the investor pursues some measure of risk diversification. If one investment fails to bring returns, others can pick up the slack.[63]

Al Qaeda employs a portfolio approach to operations. Officials have recognized that Al Qaeda needs to be right only once to achieve its expressive and instrumental goals, while security officials must be right every time.[64] Running several plots simultaneously keeps State adversaries guessing, lodging the initiative with Al Qaeda. Even if the vast majority of attacks are prevented, one catastrophic attack sends the message that Al

---

60. *See* Holder v. Humanitarian Law Project, 130 S. Ct. 2705, 2729–30 (2010); *cf.* Peter Margulies, *Advising Terrorism: Material Support, Safe Harbors, and Freedom of Speech*, 63 HASTINGS LAW JOURNAL 455, 486–93 (2012) (discussing manipulation of public opinion by terrorist groups).

61. *Cf.* Ronald J. Gilson & Robert H. Mnookin, *Disputing Through Agents: Cooperation and Conflict Between Lawyers in Litigation*, 94 COLUMBIA LAW REVIEW 509 (1994) (discussing virtues and risks of working through agents).

62. *Cf.* Matthew C. Waxman, *The Structure of Terrorism Threats and the Laws of War*, 20 DUKE JOURNAL OF COMPARATIVE & INTERNATIONAL LAW 429, 433–37 (2010) (distinguishing between "top-down" and "bottom-up" threats).

63. *See* Lee-Ford Tritt, *The Limitations of an Economic Agency Cost Theory of Trust Law*, 32 CARDOZO LAW REVIEW 2579, 2622 (2011).

64. *See* Frances Fragos Townsend, *The President's Plan, in 10 Ways to Avoid the Next 9/11*, NEW YORK TIMES, Sept. 10, 2006, § 4, 13.

Qaeda is still on the map. That message encourages further attacks and distorts government policies. Al Qaeda uses a similar approach to organizational form. It varies its structure as the need requires, equipping its personnel to leverage "evolving relationships" rather than being wed to a particular organizational structure.[65] Sticking with one organizational form would also give an advantage to Al Qaeda's adversaries.[66] Al Qaeda has adopted an approach to structure that minimizes this risk, mixing command decisions with subordinates' operational initiative. While some have argued that most terrorist acts are the product of independent, grassroots efforts,[67] that picture is decidedly incomplete. According to terrorism expert Bruce Hoffman, Al Qaeda is a "remarkably agile and flexible organization that exercises both top-down and bottom-up planning and operational capabilities."[68]

Accounts of terrorist groups as creatures of chaos are inaccurate. It turns out that terrorist groups breed bureaucracy. Like lawful organizations, terrorist groups wrestle with the ubiquitous problem of agency costs. Al Qaeda, like a State military unit, uses personnel drawn from a variety of backgrounds whom it expects to fulfill the group's mission.[69] However, operatives may have agendas of their own. For example, they may have an interest in looting civilian property or skimming money from the group and enriching themselves.[70] Alternatively, terrorist operatives may engage in *more* violence than the group's leaders find optimal, because the operatives

---

65. *See* Reid Sawyer & Michael Foster, *The Resurgent and Persistent Threat of al Qaeda*, 618 ANNALS OF THE AMERICAN ACADEMY OF POLITICAL & SOCIAL SCIENCE 197, 200 (2008).

66. *See* Abdulkader H. Sinno, *Armed Groups' Organizational Structure and Their Strategic Options*, 93(882) INTERNATIONAL REVIEW OF THE RED CROSS 311, 318 (2011) (noting that networks such as Al Qaeda are less vulnerable to State retaliation because of the mobile and dispersed nature of their leadership).

67. *See* MARC SAGEMAN, LEADERLESS JIHAD: TERROR NETWORKS IN THE TWENTY-FIRST CENTURY 23–24 (2008).

68. Hoffman, *supra* note 54, at 134.

69. Jacob N. Shapiro & David A. Siegel, *Moral Hazard, Discipline, and the Management of Terrorist Organizations*, 64 WORLD POLITICS 39, 73 (2012); *see also* John Mueller & Mark G. Stewart, *The Terrorism Delusion: America's Overwrought Response to September 11*, INTERNATIONAL SECURITY, Summer 2012 (arguing that individual defendants convicted in the United States of terrorism-related crimes were often lacking in competence and judgment); *cf.* Brahma Chellaney, *Fighting Terrorism in Southern Asia: The Lessons of History*, INTERNATIONAL SECURITY, Winter 2001–02, at 96–97 (noting, as an example of agency costs in counterterrorism, that aid to South Asian governments and non-State groups to fight terrorism has been siphoned off for other purposes).

70. Shapiro & Siegel, *supra* note 69, at 54–55.

have developed habits of violence while leaders sometimes believe that relative restraint enhances the organizational brand.[71] Bureaucratic rules and procedures can help the terrorist group address these problems.

Consider the case of Al Qaeda in Iraq (AQI). AQI was a "cohesive organization with shared personnel across 'official' names, institutional memory, embedded management practices, and permanent salaried employees."[72] Both AQI and its successor organization, the Islamic State of Iraq (ISI), took steps to enforce discipline among members.[73] For example, terrorist groups such as AQI keep copious records of the success and failure of operations, even though maintaining such records greatly enhances the risk that adversaries will obtain custody of this information and use it against these groups.[74] Groups such as AQI clearly believe that committing rules and communications to writing tightens the organization of the group, making defection or shirking more difficult. AQI required signed pledges by fighters who consented to conditions on various activities.[75] For example, AQI threatened to expel members who engaged in ordinary criminal conduct, such as looting, which would distract from the group's ideological agenda.[76] ISI instituted controls that would bring a glow to the most austere of accountants, decreeing that, "[f]or every amount paid out of [organizational] funds, the recipient is required to provide two signatures . . . one for receiving the money and another one to show how the money was spent."[77] Another ISI pronunciamento declared that "[a]ll properties, small and large, will be inventoried."[78] The ISI also required operatives to upload information on flash drives, to be "sent every week to the [group's] administrator."[79] The proliferation of flash drives and memory sticks obviously ratchets up the risk that some of the information contained in these devices will end up in the hands of the group's adversaries.[80] However, ISI apparently determined that the benefits of such a structure to group discipline outweighed those risks.

---

71. *Cf.* Mueller & Stewart, *supra* note 69, at 91 (asserting that Muslim population worldwide has been alienated by Al Qaeda's indiscriminate violence).

72. Shapiro & Siegel, *supra* note 69, at 48 n.32.

73. *Id.* at 47.

74. *Id.*

75. *Id.* at 48.

76. *Id.* at 49–50.

77. *Id.* at 50.

78. Shapiro & Siegel, *supra* note 69.

79. *Id.* at 51.

80. *Id.* at 50.

ISI also kept careful track of all of its operatives, cataloging incoming fighters, ongoing staff and "exiting brothers."[81] These internal records distinguished between the assignments of new staff, who might be suicide bombers or perform other roles.[82] This record keeping, like the ban on looting, served strategic and ideological purposes. Operatives in Iraq were often foreign nationals who had entered Iraq because ISI's practice of violence resonated with their preconceived beliefs or habits.[83] Left to their own devices, these recruits might engage in violence "for its own sake."[84] However, indiscriminate violence, like looting, could impair the group's messaging. Record keeping also enhances the propaganda capabilities of terrorist groups. In most groups, claiming credit for an attack is as important as the attack itself.[85] Claiming credit announces to the world and to other terrorist groups that the organization has "arrived." Claiming credit for violence also enhances the group's commitment: a suicide attack, for example, signals the sincerity of the attacker's beliefs and those of the organization.

One can also view a strategy relying on suicide attacks as a decision about the costs of internal monitoring. Suppose that a terrorist leader orders a conventional (non-suicide) attack. For whatever reason, the attack fizzles. The group's leadership then could have a difficult time in evaluating the causes for the attack's failure in a "noisy" environment,[86] where many factors can impede optimal execution. An attacker who survives a suboptimal attack will likely have many excuses for why the operation failed to go as planned. The leader will need to weigh those excuses before deciding on the staffing for the next attack. A suicide attack dispenses with the excuse-sifting phase, and also gives the suicide operative no exit strategy apart from outright desertion. Since that path leads to disgrace,[87] a suicide attack

81. *Id.* at 51.

82. *Id.*

83. *Id.* at 52.

84. Shapiro & Siegel, *supra* note 69.

85. *See* Abrahms, *supra* note 56.

86. *See* Shapiro & Siegel, *supra* note 69, at 73.

87. This is a particularly compelling factor when groups also provide social services and cash benefits to operatives' families. *See* Boim v. Holy Land Foundation for Relief & Development, 549 F.3d 685, 698 (7th Cir. 2008) (noting that Hamas's social service programs "mak[e] it more costly . . . to defect"); Eli Berman & David D. Laitin, *Religion, Terrorism, and Public Goods: Testing the Club Model*, 92 JOURNAL OF PUBLIC ECONOMICS 1942, 1952, 1955 (2008) (same); *see also* Justin Magouirk, *The Nefarious Helping Hand: Anti-*

is often a good way of ensuring discipline. However, making sure that the operative has sufficient ties to the organization and a "track record" of violence and ideological commitment requires some degree of organization.

B. Terrorist Networks and Global Reach

Al Qaeda displays this mix of organizational forms in its relationships with affiliated groups.[88] While Al Qaeda's core remains in Pakistan, its lack of geographic proximity to other groups is not necessarily a weakness. Network theory teaches us that physical proximity is less important when knowledge and values can be shared in other ways.[89]

Links between Al Qaeda and regional groups are synergistic along a number of axes. The Taliban/Al Qaeda link has been durable and effective because it combined the embedded localism of the Afghan Taliban with the extreme Islamist network of schools and camps based in Pakistan.[90] In other situations, regional organizations seek out Al Qaeda when State pressure has weakened the organization.[91] Allied with Al Qaeda, groups can share information on effective strategies and learn from their mistakes.[92] Al Qaeda has historically welcomed such overtures, since they assist the global group in extending its brand.[93] More sophisticated technology, including improvement in transportation and communications, has made it far easier to coordinate activities across regions.[94]

Corruption Campaigns, Social Services Provisions, and Terrorism, 20(3) TERRORISM & POLITICAL VIOLENCE 356, 358 (2008) (discussing Hamas's provision of social services).

88. For more on the strengths and weaknesses of networks, see Mette Eilstrup-Sangiovanni & Calvert Jones, *Assessing the Dangers of Illicit Networks: Why al-Qaida May Be Less Threatening Than Many Think*, INTERNATIONAL SECURITY, Fall 2008, at 11–33 (2008); *see also* Chesney, *supra* note 1, at 23–29 (discussing interaction and entropy in Al Qaeda's relationships with groups in Yemen and Somalia).

89. Stephen R. Borgatti & Rob Cross, *A Relational View of Information Seeking and Learning in Social Networks*, 49 MANAGEMENT SCIENCE 432, 436, 439, 441 (2003).

90. *See* Paul Staniland, *Organizing Insurgency: Networks, Resources, and Rebellion in South Asia*, INTERNATIONAL SECURITY, Summer 2012, at 171 (Summer 2012).

91. Daniel L. Byman, *Breaking the Bonds Between Al-Qa'ida and Its Affiliate Organizations* 14–15 (Aug. 2012), *available at* http://www.brookings.edu/~/media/research/files/papers/2012/7/alqaida%20terrorism%20byman/alqaida%20terrorism%20byman.pdf.

92. *Id.* at 15.

93. *Id.* at 13.

94. *See* Jeremy Pressman, *Rethinking Transnational Counterterrorism: Beyond a National Framework*, 30(4) THE WASHINGTON QUARTERLY 63, 64 (Autumn 2007).

Examples of this synergy abound. For example, Al Qaeda in the Arabian Peninsula (AQAP), which operates primarily in Yemen, began as a result of "direct orders" from Osama bin Laden to Al Qaeda members on the ground in that region.[95] Today, AQAP is both more "professional" in its operations and more linked to the Al Qaeda "core."[96] In North Africa, Al Qaeda of the Islamic Maghreb (AQIM) enjoys a partnership with Al Qaeda.[97] Al Qaeda's current leader, Dr. Ayman al-Zawahiri, announced a "blessed union" with AQIM, leading both groups to focus on attacking French interests.[98] In Somalia, the terrorist group al Shabab publicly pledged its loyalty to Al Qaeda.[99] Operatives trained in Afghanistan camps transferred to Somalia to provide training to Shabab members.[100] The two organizations now cooperate on a host of matters, from ideological instruction to advanced tactics.[101] Zarqawi's AQI "willingly merged" with bin Laden's group, although the latter had been weakened by the erosion of its base in Afghanistan after September 11.[102] Credible evidence indicates that members of Al Qaeda in Iraq have been assigned to "establish cells in other countries."[103]

Al Qaeda provides training for operations elsewhere. For example, the perpetrators of the London subway suicide attacks obtained training from Al Qaeda branches in Pakistan.[104] Indeed, Al Qaeda provided training in

---

95. *See* Leah Farrall, *How Al Qaeda Works: What the Organization's Subsidiaries Say About Its Strength*, 90 FOREIGN AFFAIRS 128, 132 (2011); *cf.* Byman, *supra* note 91, at 5–6 (discussing relationship between Al Qaeda and AQAP); Jane Novak, *Arabian Peninsula al Qaeda groups merge*, LONG WAR JOURNAL, Jan. 26, 2009, http://www.longwarjournal.org/archives/2009/01/arabian_peninsula_al.php (same).

96. *See* Byman, *supra* note 91, at 6.

97. *Id.*

98. *Id.*

99. *Id.*

100. *Id.* at 7.

101. *Id.*

102. Farrall, *supra* note 95, at 133; *cf.* Matthew Levitt, *Untangling the Terror Web: Identifying and Counteracting the Phenomenon of Crossover Between Terrorist Groups*, 24(1) SAIS Review 33, 38–39 (Winter–Spring 2004).

103. *See* Hoffman, *supra* note 54, at 135. The pattern of collaboration with Al Qaeda is not monolithic; members of some groups have broken away. *See* Byman, *supra* note 91, at 7–8 (discussing Egypt's Gama al-Islamiya, many of whose members renounced violence after influence of Al Qaeda led to widely criticized 1997 attack on tourists at Luxor).

104. *See* Hoffman, *supra* note 54, at 138; Anthony N. Celso, *Al Qaeda's Post-9/11 Organizational Strategy: The Role of Islamist Regional Affiliates*, 23 MEDITERRANEAN QUARTERLY 30, 35 (2012); *cf.* Pressman, *supra* note 94, at 65 ("[f]undraising, recruitment . . . and training may take place in many countries simultaneously for transnational groups").

Afghanistan, Pakistan and Yemen to as many as three thousand violent extremists from the United Kingdom, who subsequently returned, "embedd[ed] themselves" in communities and developed plans for further attacks.[105] While discrimination and alienation from the mainstream in the United Kingdom and elsewhere may have facilitated additional recruitment, "much of the terrorist threat in the United Kingdom today stems from deliberate, long-standing subversion by al Qaeda."[106] Al Qaeda–linked networks released videotaped martyrs' wills.[107] Other plots, such as the conspiracy to target transatlantic passenger aircraft in 2006, also have ties to Al Qaeda networks in Pakistan or Yemen.[108] Groups such as Hezbollah have global networks that attract financing and recruit new members.[109] Moreover, some terrorist groups have strong links to transnational criminal enterprises that share the proceeds of drug trafficking, kidnapping and prostitution.[110]

Groups partnering with Al Qaeda buy into a distinctive operational focus. While many groups have local agendas, groups under the Al Qaeda umbrella must agree to pursue attacks on Western interests.[111] The attacks on Western interests are a signature element of Al Qaeda; perpetuating these attacks allows groups under the Al Qaeda umbrella to "stay on mes-

---

105. *See* Hoffman, *supra* note 54, at 138.

106. *Id.*

107. Celso, *supra* note 104, at 35.

108. *Id.*

109. *See* Levitt, *supra* note 102, at 35. My point here is not that Hezbollah is affiliated with Al Qaeda, but that Al Qaeda may emulate Hezbollah's worldwide financial activities. *See* Jonathan M. Winer, *Countering Terrorist Finance: A Work, Mostly in Progress*, 618 ANNALS OF THE AMERICAN ACADEMY OF POLITICAL & SOCIAL SCIENCE 112, 116 (2008) (discussing Al Qaeda's funding connections in Saudi Arabia).

110. *See* Phil Williams, *Terrorist Financing and Organized Crime: Nexus, Appropriation, or Transformation?*, *in* COUNTERING THE FINANCING OF TERRORISM 126, 138–39 (Thomas J. Biersteker & Sue E. Eckert eds., Routledge 2008) (describing involvement of LTTE in heroin trade, human trafficking, gun running and extortion).

111. Farrall, *supra* note 95, at 133; *cf.* Byman, *supra* note 91, at 11 (noting that "common consequence of the embrace of an [Al Qaeda] label is for a group to seek out Western targets within a group's theater of operations"); Pressman, *supra* note 94, at 65 (discussing proliferation of Osama bin Laden's strategy of attacks on Western targets). David H. Petraeus, the former Director of the Central Intelligence Agency, recently told congressional committees that Al Qaeda appears to have influenced the targeting of the American diplomatic mission in Benghazi, Libya that resulted in the deaths of Ambassador J. Christopher Stevens and three other Americans. *See* Eric Schmitt, *Petraeus Says U.S. Tried to Avoid Tipping Off Terrorists After Libya Attack*, NEW YORK TIMES, Nov. 17, 2012, at A10.

sage."[112] Moreover, Al Qaeda insists on specific approval for attacks outside a subsidiary's regional base.[113] For example, when a Danish newspaper published caricatures of the Prophet Muhammad, Al Qaeda asked its Iraqi branch to carry out attacks on Danish interests.[114] U.S. officials believe that Hezbollah operatives played a significant role in the July 2012 attack in Bulgaria on a bus carrying Israeli tourists.[115] In addition, Al Qaeda requires certain operational modalities for attacks outside a branch's region. Al Qaeda pushes suicide attacks and patterned attacks on particular kinds of targets, such as public transportation, government structures and infrastructure.[116] This layer of specific operational control demonstrates Al Qaeda's organizational contours and confirms its existence and functioning as a "united front."[117] Al Qaeda also has structural mechanisms that ensure communication and guidance. It uses information committees that are tied to senior leadership and operational planners.[118]

A networked approach driven by an anti-Western strategic focus has many advantages for Al Qaeda. Shared ideology lessens the likelihood of deterring the group through ordinary law enforcement or negotiation. Suicide bombers will not blink at the prospect of arrest and trial. Rather, involvement with the legal system confers another opportunity for the attackers to brand themselves as martyrs.[119] In addition, networks such as Al Qaeda and its affiliates are far less amenable to negotiation than territory-based groups. Groups that control territory within a single State may on occasion be a party to successful negotiations, as the IRA demonstrated.[120] Such movements may gain a stake in negotiations, as they seek to ease State pressure on their territorial base.[121] In contrast, the disaggregation of terri-

112. Farrall, *supra* note 95, at 133.

113. *Id.* at 134.

114. *Id.*

115. *See* Nicholas Kulish, *Despite U.S. Fear Hezbollah Moves Openly in Europe*, NEW YORK TIMES, Aug. 16, 2012, at A1.

116. *See* Farrall, *supra* note 95, at 135.

117. *Id.* at 133.

118. *Id.* at 135.

119. *Cf.* Christopher Slobogin, *A Jurisprudence of Dangerousness*, 98 NORTHWESTERN UNIVERSITY LAW REVIEW 1, 44–46 (2003) (noting intransigence yielded by ideological commitments of members of terrorist networks); Michael A. Newton, *Exceptional Engagement: Protocol I and a World United Against Terrorism*, 45 TEXAS INTERNATIONAL LAW JOURNAL 323, 362 (2009) (noting that terrorist groups are often "undeterred by existing criminal law").

120. *See* Pressman, *supra* note 94, at 68–70.

121. *Id.* at 69.

tory and operations in transnational networks mean that those groups lack a "return address." Since transnational groups can readily shift their operations,[122] State pressure is not an effective deterrent. The absence of a general deterrent only exacerbates the risk of armed conflict from transnational groups, and makes specific deterrence or incapacitation of the group's operatives all the more imperative.[123]

On the basis of this analysis of terrorist and network organization, targeting of an Al Qaeda affiliate is permissible on a showing that Al Qaeda exerts a strategic influence on the targeted group. A State considering targeting members of the Al Qaeda subsidiary should have a reasonable basis for believing that Al Qaeda guides some or all of the group's choice of targets. Mere subscription to an ideology is not enough—nor is financing, although financing can be one factor contributing to an inference of strategic influence. Policymakers should have a reasonable belief that Al Qaeda has leveraged money, recruits, training or expertise to encourage the affiliate's targeting of Western interests or moderation in the targeting of Muslim civilians. Ongoing correspondence or exchanges of information about targeting or operations should give rise to an inference that such influence is present. Al Qaeda's role in the training of an affiliate's recruits should also have evidentiary significance.[124] No rigid hierarchy need be shown—indeed, as we have seen, the case law from transnational tribunals has often required less hierarchy than meets the eye.[125]

IV. CONCLUSION

One need not read the modern jurisprudence defining an OAG as being limited to groups with headquarters, fully functioning logistics or ironclad discipline. While the ICTY decisions include language setting out these criteria, the facts of the cases are actually far more ambiguous. In judgments

122. *Id.* at 70.

123. *But see* Eilstrup-Sangiovanni & Jones, *supra* note 88, at 36–37 (noting that network form can create security problems because of looser control by leadership and reliance on local operatives infiltrated by law enforcement, while acknowledging that security issues have not necessarily impaired groups' abilities to cause massive harm to civilians).

124. *See* Haradinaj, *supra* note 53, ¶ 86 (discussing importance of training).

125. Of course, targeting suspected terrorists is only one aspect of an effective counterterrorism strategy. Aid that reaches needy individuals and groups can help goodwill toward the West and counter the appeal of terrorist groups. *See* Aloke Chakravarty, *Feeding Humanity, Starving Terror: The Utility of Aid in a Comprehensive Antiterrorism Financing Strategy*, 32 WESTERN NEW ENGLAND LAW REVIEW 295, 325–29 (2010).

such as *Limaj*, the ICTY found organization when traditional elements were equivocal. The ICTY jurisprudence and the analysis of many commentators point toward a more pragmatic approach.

That said, terrorist organizations often reveal surprisingly strong elements of organization. Like other entities, terrorist groups devise mechanisms to deal with the problem of agency costs. They monitor, assess and document performance of their personnel, and make appropriate changes when needed. These measures exist even when they appear to endanger the groups' security.

The versatile approach to organization that marks terrorist groups within a State also holds true for transnational networks such as Al Qaeda. Al Qaeda operates in a synergistic fashion with regional groups. Many groups have received training from Al Qaeda's core feeder sources of schools and camps, and have sworn allegiance to Al Qaeda to enhance their appeal and access to resources. Direct operational control is rarely present. However, strategic influence, including a focus on targeting Western interests, is common. When such strategic influence can be shown, the definition of an OAG is sufficiently flexible to permit targeting across borders.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Geography of Armed Conflict: Why it is a Mistake to Fish for the Red Herring

Geoffrey S. Corn

89 INT'L L. STUD. 77 (2013)

Volume 89 2013

Geography of Armed Conflict: Why it is a Mistake to Fish for the Red Herring

Geoffrey S. Corn[*]

I. INTRODUCTION

Identifying a framework for assessing the permissible geography of armed conflict must be driven by both strategic and legal considerations. Armed conflict by its very nature manifests the exercise of national power implicating the most fundamental aspect of sovereignty: the right and obligation of the State to protect itself from internal or external threat.[1] Categories of armed conflict[2] and their associated legal regimes evolved in response to this reality. Up until recently, almost all threats functionally sufficient in nature and magnitude to necessitate a full–blown military response (the use of military force to execute combat operations, as opposed to constabulary

* Presidential Research Professor of Law, South Texas College of Law; Lieutenant Colonel, U.S. Army (Ret.). Special thanks to my research assistant, Joel Glover, whose devotion to accomplishing this mission undoubtedly mirrored the type of devotion he brought to his duties as a platoon leader and a battalion effects coordinator in Iraq, and as co–captain of Army football. The opinions shared in this paper are those of the author and do not necessarily reflect the views and opinions of the U.S. Naval War College, the Department of the Navy, or Department of Defense.

1. Deni Elliott, *Terrorism, Global Journalism and the Myth of the Nation-State*, 19 JOURNAL OF MASS MEDIA ETHICS: EXPLORING QUESTIONS OF MEDIA MORALITY 29 (2004).

2. Dietrich Schindler, *The Different Types of Armed Conflicts According to the Geneva Conventions and Protocols*, 63 THE HAGUE ACADEMY COLLECTED COURSES 131 (1979).

support operations)[3] took the form of hostilities between two or more States (characterized by international law as international armed conflicts), and bringing into force the full corpus of the law of armed conflict (LOAC), or internal dissident or insurgent threats involving hostilities between State forces and organized armed groups (characterized by international law as non–international armed conflicts, and bringing into force a less comprehensive albeit substantial body of LOAC regulation). Accordingly, LOAC responded to these two "types" of armed conflicts[4] with a continual and important progression of regulatory norms applicable to both categories.[5] These norms, and the constant progression of their content and applicability, were and are intended to balance the strategic needs of the State with the humanitarian objectives that have always animated conflict regulation.[6]

It is debatable, however, whether these two categories of armed conflict were from inception underinclusive, in the sense that they failed to account for situations of armed hostilities falling outside their scope.[7] This underinclusiveness is illustrated by U.S. military history. Examples of combat operations that would fail to fit nicely within these two dominant categories of armed conflict include the U.S. participation in the multinational response to the 1900 Boxer Rebellion in China; the 1916 U.S. punitive raid against Pancho Villa in Mexico; and the U.S. and Allied intervention in the Russian Civil War (which actually resulted in a U.S. force presence on Russian soil through 1921, long after the end of World War I).[8] These exam-

3. *See* Keith Robert Lovejoy, *A Peacekeeping Force for Future Operations: Another Reassessment of the Constabulary Force Concept* (2003), *available at* http://www.dtic.mil/dtic/tr/fulltext/u2/a414134.pdf.

4. Sylvain Vité, *Typology of Armed Conflicts in International Humanitarian Law: Legal Concepts and Actual Situations*, 91 INTERNATIONAL REVIEW OF THE RED CROSS 1, 82–86 (2009) (discussing the different types of armed conflict) [hereinafter Vité].

5. JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, ICRC, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW (2005), *available at* http://www.icrc.org/customary-ihl/eng/docs/v1_cha_chapter1_rule1 (last visited Aug. 9, 2012).

6. ICRC, INTRODUCTION TO THE LAW OF ARMED CONFLICT: BASIC KNOWLEDGE, *available at* http://www.icrc.org/eng/assets/files/other/law1_final.pdf (last visited Sept. 9, 2012) and Rupert Ticehurst, *The Martens Clause and the Laws of Armed Conflict*, 317 INTERNATIONAL REVIEW OF THE RED CROSS 125 (1997).

7. Geoffrey S. Corn, *Hamdan, Lebanon, and the Regulation of Hostilities: The Need to Recognize a Hybrid Category of Armed Conflict*, 40 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 295, 296–97 (2007) [hereinafter Corn].

8. Michael Parenti, *Rulers of the Planet: Why US Leaders Intervene Everywhere*, 5 GLOBAL DIALOGUE (2003), *available at* http://www.worlddialogue.org/print.php?id=220.

ples illustrate that in practice armed conflict has never been statically confined to the two "types" that became the dominant focus of conflict regulation following World War II. More important for the purposes of this essay, these two categories of armed conflict have not been the definitive standard for assessing the geographic scope of combat operations.[9]

The post–World–War–II bipolar strategic environment did, however, reinforce the binary nature of armed conflict typology—and with it the assumption that the nature of the armed conflict included an implicit geographic scope limitation. Wars were generally confined to the geography of one or two States. Even the limited inter–State armed conflicts of the period lacked the widespread geographic range of operations that defined the two world wars.[10] Instead, as a result of the immense perceived risks associated with conflagration, most armed conflicts were generally "self–contained" events. Nonetheless, the perceived U.S. need for global engagement capability was a primary characteristic of national security policy. The Cold War was indeed defined by the strategic capacity to meet any threat, in any location, in the form in which it presented itself.[11] While history was kind to spare the world from the global consequence of the Cold War turning hot, the practice of forward deployment and global engagement indicates that had this occurred, the conflict would have been worldwide.

The end of the Cold War blew the lid off of a pot that had been simmering for the entire period: the threat of international terrorism. While during the Cold War terrorism was generally treated as a subtext to the global bipolar struggle,[12] it soon came into its own as a national security threat. While the risk associated with international terrorism became increasingly apparent, the modality for protecting against this risk was anything but apparent. During the decade preceding September 11, 2001, this situation manifested itself in tremendous operational uncertainty, especially for the armed forces. Counterterrorism was viewed as one of the many potential military missions that fell into the category of "Low Intensity Con-

9. Department of the Navy, MCDP 1, WARFIGHTING (1997).

10. *See generally* MARTIN GILBERT, THE FIRST WORLD WAR: A COMPLETE HISTORY (1994); RONALD STORY, CONCISE HISTORICAL ATLAS OF WORLD WAR II: THE GEOGRAPHY OF ARMED CONFLICT (2005).

11. *See* ROGER S. WHITCOMB, THE COLD WAR IN RETROSPECT: THE FORMATIVE YEARS 182–84 (1998).

12. WAYNE C. MCWILLIAMS & HARRY PIOTROWSKI, THE WORLD SINCE 1945: A HISTORY OF INTERNATIONAL RELATIONS 1 (6th ed. 2005).

flict" or "Military Operations Other Than War."[13] U.S. military doctrine did not, however, address the legal characterization of such missions. Consequently, military counterterrorism was generally understood as military support to international law enforcement,[14] although military action occasionally took the form of combat operations (such as the cruise missile attack against suspected al Qaeda targets in response to the African embassy bombings).[15] Whatever the legal characterization, one thing seemed increasingly clear: the scope of operations would, like virtually all other military missions, be threat driven.

How the U.S. military response to the terrorist attacks of September 11 impacted the typology of armed conflict is arguably yesterday's news, at least for the United States. While certainly not an accepted theory of armed conflict, the term "transnational armed conflict" (TAC)—indicating a non–international armed conflict, and its accordant LOAC rules, occurring outside the territory of the responding State—has gained increasing traction in the United States and abroad to denote an armed conflict against a non–State threat in various global environments.[16] This usage suggests a broader recognition of the under–inclusiveness of the binary armed conflict framework. There is also no question that assertion of a hybrid category of armed conflict—whether characterized as TAC or an internationalized Common Article 3 armed conflict—has generated substantial consternation that is in large measure the result of the link between TAC and the broad geographic scope of military operations it ostensibly legitimizes.[17]

---

13. *See* James N. Miller Jr., Assistant Secretary of Defense for Special Operations / Low-Intensity Conflict, *available at* http://policy.defense.gov (last visited Sept. 8, 2012).

14. Joint Publication 3-26, COUNTERTERRORISM, (2009), *available at* http://www.dtic.mil/doctrine/new_pubs/jointpub_operations.htm.

15. LAUREN PLOCH, CONGRESSIONAL RESEARCH SERVICE, COUNTERING TERRORISM IN EAST AFRICA: THE U.S. RESPONSE 1–2 (2010).

16. Vité, *supra* note 4, at 88; Corn, *supra* note 7; *see* Geoffrey S. Corn & Eric T. Jensen, *Transnational Armed Conflict: A "Principled" Approach to the Regulation of Counter-Terror Combat Operations*, 42 ISRAEL LAW REVIEW 1, 33–34 (2009) (discussing how the continued evolution of TAC, or the acts of "war" carried out by States that attack non-State targets outside of their boundaries, must preserve "the fundamental balance between authority and obligations that lies at the core of the LOAC" to preserve its legitimacy as it becomes more common) [hereinafter Corn & Jensen].

17. Jennifer C. Daskal*, The Geography of the Battlefield: A Framework for Detention and Targeting Outside the 'Hot' Conflict Zone*, 161 UNIVERSITY OF PENNSYLVANIA LAW REVIEW (forthcoming 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2049532 (last visited Sept. 8, 2012) [hereinafter Daskal]; Mary Ellen O'Connell, *Defining Armed Conflict*, 13 JOURNAL OF CONFLICT SECURITY LAW 393 (2008); George Monbiot, *A*

The debate over conflict typology raises this question: is the TAC concept inherently invalid? Put another way, is the invocation of unrestricted geographic scope for an armed conflict against a non–State opponent the true focal point of objection to this typology? The latter proposition may explain why some experts now seek to impose an implied geographic limitation on the conduct of operations within the framework of TAC—such as an implied constraint to what some scholars have labeled "hot zones" of military operations.[18] Ultimately, however, seeking to identify and impose a geographic restriction detached from the threat dynamics triggering the use of combat power is a false solution to the concerns of operational overbreadth associated with TAC. Such limitation is a futile endeavor, for the developing axiomatic reason that once a State commits to the use of force as a remedy against such a transnational non–State threat—like all other conflicts in history—the dynamics of the threat itself will be the predominant consideration in defining the scope of operations.

This latter premise frustrates some international law scholars. They insist that the first step in defining the geographic scope of military operations is to assess the internationally permissible geography of armed conflict. Strategy, they posit, must yield to international legal constraint.[19]

This is undoubtedly the "correct" ideological starting point: law imposes its own geography—the geography of permissible policy maneuver space. Decisions related to when, where and how to use instruments of national power are not made in a legal vacuum. Rather, domestic and international law significantly impact these decisions. Legal advisors inform policy decisions by providing the policymaker with the left and right boundaries of permissible conduct. This framework is far more complex on the more specific issue of geography of armed conflict. Even assuming international law categorically constrains permissible strategy options (an assumption that ignores the reality that States periodically choose to violate international law in order to achieve vital national security objectives), the relevant law must be unequivocal. On the question of conflict geography,

---

Wilful Blindness, THE GUARDIAN, Mar. 11, 2003, *available at* http://www.guardian.co.uk./world/2003/mar/11/usa.iraq.

18. Daskal, *supra* note 17; Ashley Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VIRGINIA JOURNAL OF INTERNATIONAL LAW 483 (2012) [hereinafter Deeks].

19. Michael N. Schmitt, *Asymmetrical Warfare and International Humanitarian Law*, 84 AIR FORCE LAW REVIEW 1, 35–36 (2008).

however, this is not the case. It involves a complex intersection of *jus ad bellum*,[20] neutrality[21] and *jus in bello* principles.[22]

None of these sources categorically define a geographic constraint on the execution of combat operations within the context of an ongoing non–international armed conflict. Instead, they combine to provide a general outline of acceptable State action, sometimes by analogy (such as the effort to extend neutrality principles to the inapposite context of non–international armed conflict), or sometimes more directly (such as the invocation of the principle of military necessity as a source of authority to adopt a threat–based scope of combat operations). On the geography of conflict question, the net outcome is anything but an unequivocal international legal standard that nullifies the validity of a —driven scope of military operations. This is unsurprising. The entire TAC concept is an evolution of existing LOAC principles, as is the exercise of national self–defense in response to a transnational non–State threat. Thus, international law has yet to settle on an issue as complex as permissible geography of operations conducted in response to the threat of international terrorism.

Seeking to identify some legally mandated geographic boundary for armed conflict of any type is, thus, a genuine *Red Herring*.[23] Armed conflict is a threat–driven concept, arising when the threat necessitates resort to combat power, and extending to wherever the operational and tactical opportunity to produce a militarily valuable effect on the enemy arises. There are examples of States choosing not to expand the scope of conflicts simply because such an opportunity arose. However, other factors impact such decisions, and it would be an error to equate decisions to refrain from exercising authority with an inherent legal prohibition against such exercise.

The scope of TAC—like that of any armed conflict—must be threat driven for a reason. Admittedly, there exists a perceived and actual risk of

---

20. Deeks, *supra* note 18.

21. INTERNATIONAL COMMITTEE OF THE RED CROSS, THE LAW OF ARMED CONFLICT NEUTRALITY, *available at* http://www.icrc.org/eng/assets/files/other/law8_final.pdf ("Belligerent States have a number of duties. They must establish a neutrality policy ensuring respect for neutral space, in particular that armed forces involved in the conflict do not enter neutral space and that neutral States are not affected by the collateral effects of hostilities.").

22. Most notably the principle of military necessity as a justification for taking the fight to the enemy.

23. Targeting Operations with Drone Technology: Humanitarian Law Implications (Mar. 25, 2011), *available at* http://www.law.columbia.edu/ipimages/Human_Rights_Institute/BackgroundNoteASILColumbia.pdf.

an overzealous and overbroad assertion of LOAC–based authority to attack and disable threat operatives inherent in the combined effect of TAC as a theory of armed conflict typology and a threat–driven scope interpretation. Nonetheless, States must avoid attempts to identify or impose some *per se* geographic limitations on this type of armed conflict. Any authority overreach (invoking the power to incapacitate through an application of LOAC principles), triggered by extending the concept of armed conflict to transnational non–State threats, will be more effectively mitigated by focusing on the traditional dynamics of lawful wartime action and tailoring or adjusting traditional sources of LOAC authority to meet the unique challenges of this type of armed conflict. Chief among these particular challenges are, one, ensuring that the targeting process adequately accounts for the complexity of threat identification in this inherently unconventional environment; and two, ensuring that preventive detention processes sufficiently address the unique scope and nature of this type of armed conflict. Focusing on these two practical challenges will produce a better balance between national security realities and the individual interests of potential objects of State action than would be achieved by attempting to confine that action to an arbitrary "hot zone."

II. INTERNATIONAL TERRORISM, NATIONAL SECURITY AND THE GLOBALIZATION OF NON–INTERNATIONAL ARMED CONFLICT

It is self–evident that a principal function of any government is to protect State interests from external and internal threats.[24] To do so, leaders leverage the various components of national power, ideally in a synchronized manner that maximizes strategic success by achieving the protective objective as efficiently as possible.[25] Military power is a key tool in the national security arsenal, often providing strategic decision makers with unique capabilities to inflict devastating blows to disrupt or disable threat capabilities.

For the United States, the ability to leverage military power effectively is rooted in its very origins. A nation born of conflict, and unified in part

24. President Barack Obama, Nobel Peace Prize Acceptance Speech (Dec. 10, 2009), *available at* http://www.nobelprize.org/nobel_prizes/peace/laureates/2009/obama-lecture_en.html.

25. *See* President George W. Bush, The National Security Strategy of the United States (Sept. 2002), *available at* http://georgewbush-whitehouse.archives.gov/nsc/nss/2002/nss3.html [hereinafter National Security Strategy].

because of the recognized need to "perfect" our collective ability to provide for a common defense, the use of military power to secure national security objectives has been a constant theme of our national narrative. In this sense, the utilization of military power to contribute to the national objective of neutralizing the capacity of international terrorism is not especially remarkable. Indeed, it seems more noteworthy that it took the devastating attacks of September 11 for national leaders to become overt and unapologetic about this utilization, even though it is well established that such use was ongoing prior to that date.[26]

No single national security policy shift in recent memory has produced more legal controversy than the overt, robust and ongoing use of a State's military power as an international counterterrorism tool.[27] This is equally unremarkable for two primary reasons. First, never before had the United States engaged in an ongoing military campaign of this magnitude and duration against a non–State opponent operating in various locations throughout the globe. Second, and perhaps more importantly, is the consistent invocation of authority derived from a situation of armed conflict to provide the legal foundation for these military operations. This has produced a profound expansion of national authority to seek out and incapacitate members of terrorist organizations falling within the scope of what the United States considers the "enemy"—defined by the authority to kill as a measure of first resort and subject captives to long–term preventive detention.[28]

When the Bush administration originally coined the phrase "Global War on Terror" (GWOT), it was intended to put the terrorist enemy on notice that no longer were they functionally immune from the powerful U.S. combat arsenal. However, it also unleashed a decade long barrage of

---

26. Stephen J. Schulhofer, Statement to the National Commission on Terrorist Attacks upon the United States (Dec. 8, 2003), *available at* http://govinfo.library.unt.edu/911/hearings/hearing6/witness_schulhofer.htm.

27. Jules Lobel, *The Preventive Paradigm and the Perils of Ad Hoc Balancing*, 91 MINNESOTA LAW REVIEW 1407, 1407–8 (2007); Monbiot, *supra* note 17.

28. Corn & Jensen, *supra* note 16, at 45–46; John Brennan, Assistant to the President for Homeland Security and Counterterrorism, Remarks at the Program on Law and Security Harvard Law School: Strengthening Our Security by Adhering to Our Values (Sept. 16, 2011), http://www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an [hereinafter Brennan Speech]; Eric H. Holder Jr., Department of Justice Attorney General, Northwestern University School of Law, Speech on Targeted Killing (Mar. 5, 2012), http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-1203051.html.

controversy, driven in large measure by the suggestion that this new "war" lacked any geographical limitation. Unlike wars of the recent past, all of which were conducted within a *de facto* geographically confined battlespace, the United States would, according to this new theory, take the fight to the enemy—an enemy so unconventional that this might include locations without even the slightest link to a theater of "active" combat operations, areas commonly characterized as "hot zones" today. Although President Obama abandoned the GWOT moniker, his administration nonetheless continues to strike targets of opportunity when and where they emerge, embracing the same threat–based scope of combat operations.[29]

In practice, these operations have never come close to matching the extreme rhetoric of power assertion invoked by opponents of the armed conflict with al Qaeda. The United States has never engaged in a cavalier assertion of combat power into the territory of a functioning State.[30] Opponents to the GWOT concept like to erect the straw man of a U.S. attack in the streets of Berlin, London, Paris or Zurich to demonstrate the consequences of a geographically unconstrained armed conflict against an unconventional terrorist enemy. In reality, however, the actual scope of combat operations has always been much more constrained by the (at least implicit) recognition of sovereignty.

Nonetheless, the concept of armed conflict of international scope conducted against a loosely organized non–State opponent—a typology of armed conflict resulting in the increasingly common characterization of "transnational armed conflict,"—certainly creates the perception, if not the reality, of authority overreach. The central theme of this theory is that the nature of the struggle justifies invoking and applying LOAC–based authorities, while at the same time the dispersed and unconventional nature of the "enemy" necessitates taking the fight to where the attack opportunity arises.

It cannot, however, be disputed that TAC represents a major shift in the conventional understanding of armed conflict typology.[31] Prior to Sep-

29. Laurie R. Blank, *After "Top Gun": How Drone Strikes Impact the Law of War*, 33 UNIVERSITY OF PENNSYLVANIA JOURNAL OF INTERNATIONAL LAW 675, 675–76 (2012) ("In 2010, the United States launched 118 drone strikes in Pakistan, an exponential increase over past years. In a broader view, in 2009, the U.S. Army reported a 400% increase in drone flight hours over the previous ten years. Drones are regularly used in combat operations in Afghanistan and Libya, and have been used to launch targeted killings in Somalia and Yemen.").

30. Deeks, *supra* note 18.

31. Vité, *supra* note 4.

tember 11, these conflicts were almost always confined geographically, rarely if ever raising the question of their legitimacy.[32] When they spilled into the territory of neighboring States, no significant debate was ever generated over the legally permissible "zone" of operations. This is no longer the case. Instead, primarily as the result of U.S. military operations against al Qaeda, there is an increasing tendency to assert that *even if* it is possible for the United States to be engaged in an armed conflict against this terrorist enemy, that conflict must be confined to "hot zones" of combat, most notably Afghanistan.[33] This assertion, however, fails to recognize the strategic imperative that drove the development of this TAC typology. It was precisely the need to take this fight to the unconventional enemy—wherever the threat arose—that generated the assertion of an internationalized non–international armed conflict.

III. THE RELATIONSHIP BETWEEN THE TERRORIST THREAT, TRANSNATIONAL ARMED CONFLICT AND GEOGRAPHY OF WAR

Prior to September 11 and the advent of TAC, there was virtually no discourse on the permissible geographic scope of armed conflict. This is unsurprising, considering almost all armed conflicts of this period were internal, or relatively confined inter–State conflicts.[34] Even when internal armed conflicts "spilled over" into neighboring territories, no State asserted the authority to conduct "global" operations against the non–State insurgent enemy. Use of the term "Global War on Terror" fundamentally altered the existing paradigm. Suddenly, a State was invoking the authority to engage what it determined were belligerent operatives wherever the opportunity to do so arose. U.S. global reach and dominant combat capability made it clear that this new enemy could not afford the risk of "basing" operations out of operational clusters confined to one geographic area. Because dispersion had to, by necessity, become the *modus operandi* of this new enemy,[35]

---

32. *Id.*; Corn, *supra* note 7.

33. Mary Ellen O'Connell, *The Myth of Pre-emptive Self-Defense*, ASIL Task Force on Terrorism (Aug. 2002), *available at* http://www.asil.org/taskforce/oconnell.pdf [hereinafter O'Connell].

34. Balakrishnan Rajagopal, *Invoking the Rule of Law: International Discourses*, *in* CIVIL WAR AND THE RULE OF LAW 48–53 (Agnes Hurwitz & Reyko Huang eds., 2008).

35. Manuel Almeida, *What's New in Al-Qaeda's Suicide Bombings?*, THE MAJALLA: THE LEADING ARAB MAGAZINE (Jun. 17, 2010), *available at* http://www.majalla.com/eng/2010/06/article5567539.

it inherently drove operations to extend beyond the "hot zone" of Afghanistan.[36]

Of course, it also fueled criticism of the armed conflict characterization. Critics, relying on the "organization" and "intensity" test for assessing the existence of non–international armed conflict adopted in the *Tadic* appeals judgment by the International Criminal Tribunal for the former Yugoslavia, insisted that TAC was a legal nullity.[37] In contrast, the United States has adopted more of a totality–of–the–circumstances approach to assess the existence of armed conflict, relying on the intense risk presented by al Qaeda and that organization's objective of inflicting harm on the United States and its interests wherever and whenever possible to offset the organization element of the *Tadic* test.[38] Such an approach is justified when the effectiveness of operations against an opponent disables the ability of that opponent to manifest traditional organizational characteristics. Indeed, proponents of TAC (a typology of armed conflict frequently associated with this author) implicitly understand that a strict two–prong test for assessing armed conflict produces a perverse windfall for the transnational terrorist enemy: as their operations become more unconventional and dispersed, the authority of the State to press the attack dissipates. Recent speeches by Obama administration officials seem to indicate that the assessed risk of future terrorist attacks is driving the decision to mount unrelenting pressure on al Qaeda.[39] Depriving the State of legal freedom of maneuver to press the advantage against a degraded non–State enemy is ultimately inconsistent with its strategic and operational imperative. At a minimum, it raises the complex issue of assessing the point at which a non–international armed conflict recedes back into a category of non–conflict and nullifies LOAC applicability—an issue lacking clear and consistent standards.[40]

---

36. President Barack Obama, *supra* note 24.

37. Vité, *supra* note 4.

38. Brennan Speech, *supra* note 28 ("This Administration's counterterrorism efforts outside of Afghanistan and Iraq are focused on those individuals who are a threat to the United States, whose removal would cause a significant—even if only temporary—disruption of the plans and capabilities of al-Qa'ida and its associated forces."); *see also* Laurie Blank & Geoffrey S. Corn, *Losing the Forest for the Trees: Syria, Law and the Imperatives of Conflict Recognition,* 46 VANDERBILT JOURNAL OF TRANSNATIONAL LAW __ (forthcoming, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2029989.

39. Brennan Speech, *supra* note 28.

40. Vité, *supra* note 4 (discussing the lack of standards defining when a non-international armed conflict recedes back into a category of non-conflict).

Where the United States presses this advantage has been and remains the other major source of consternation with the TAC concept. Critics assert an inherent invalidity to a claim of armed conflict authority that exceeds the geographic bounds of a "hot zone" of operations.[41] While tactical spillover operations into contiguous States may be tolerable in limited circumstances, extending combat operations to the territory of States far removed from a traditional battlespace is condemned as the ultimate manifestation of an overbroad conception of armed conflict. This criticism cuts to the core of the TAC concept. Expansive geographic scope was the very genesis of TAC, an invocation of LOAC principles to address a transnational non–State belligerent threat.[42] What these criticisms seem to overlook is a critical strategic foundation for TAC itself: the relationship between the scope of counterterror military operations and the evolution of the TAC concept reveals that like other evolutions of armed conflict typologies, threat dynamics and strategic realities drove the law applicability assessment, and not vice versa.

The U.S. response to the September 11 terrorist attacks indicated the intent to leverage military power to maximum effect whenever and wherever the opportunity arose.[43] Employing combat power in a manner indicative of armed conflict—by targeting terrorist operatives as a measure of first resort—would not be the exclusive modality to achieve this objective. However, unlike previous counterterror efforts it did become a significant, and in many cases primary, modality. Of course, selecting between military force and other capabilities involved a complex assessment of a variety of considerations, including the feasibility of alternate means to disable the threat—a classic illustration of national security policy making. What was clear, however, was that the nature of the threat drove a major shift in the response modality.

While the TAC typology seemed to defy accepted international law categorizations of armed conflict, it was never really remarkable. National security strategy is always threat driven: intelligence defines the risk created by various threats; and strategy is developed to prioritize national effort to protect the nation from these threats, including defining the tools of national power that will be leveraged to achieve this objective. When national

41. O'Connell, *supra* note 33; Daskal, *supra* note 17, at 32–33.

42. *See* Corn & Jensen, *supra* note 16.

43. Philip Alston, Jason Morgan-Foster & William Abresch, *The Competence of the UN Human Rights Council and its Special Procedures in Relation to Armed Conflicts: Extrajudicial Executions in the 'War on Terror'*, 19 EUROPEAN JOURNAL OF INTERNATIONAL LAW 183 (2008).

security policy makers determine that military power must be used as one of these tools, this is translated into a military mission. That mission is then refined in the form of military strategy, which seeks to identify threat vulnerabilities and match combat capabilities to address them.[44] Once again, the nature of the threat becomes the dominant driving force in this strategic analysis. Thus, when the threat capability and/or vulnerability is identified outside a "hot zone," it in no way nullifies the imperative of addressing the threat. In short, as others have noted, once the armed conflict door is open, threat–based strategy—focusing military action in response to threat dynamics in order to destroy or disable threat capabilities—is essentially opportunity driven: the conflict follows the belligerent target.[45]

In conventional inter–State armed conflict, this process is almost axiomatic. One need only consider events such as the sinking of the *Bismarck* in the South Atlantic during the opening phase of World War II[46] or the "small war" in East Africa between Great Britain and Germany during World War I.[47] These episodes, like countless others throughout history, indicate that the scope of armed conflict is threat driven. But the more unconventional the threat becomes, the less comfortable this concept feels. When non–international armed conflicts were almost exclusively internal in nature, this produced very little concern. It is a mistake, however, to assume this was the result of some inherent international legal invalidity of extending such conflicts beyond the territory of one State or perhaps the border regions of geographically contiguous States. Instead, like all armed conflicts, it was the combined impact of threat dynamics and diplomatic and policy considerations that drove the natural geographic constraint associated with internal armed conflicts. Indeed, examples of cross–border spillover operations bolster this conclusion. From Vietnam, to Turkey, to South Africa, to Angola, to Rwanda, to Afghanistan, when States perceived the strategic necessity of expanding an internal armed conflict into the ter-

---

44. Joint Publication 3-01, Countering Air and Missile Threats (Mar. 23, 2012), *available at* http://www.dtic.mil/doctrine/new_pubs/jp3_01.pdf ("Development of the area air defense plan and planning the defensive counter air operations involves integrating friendly force capabilities and limitations against adversary vulnerabilities to achieve optimum results in a dynamic tactical environment.").

45. Kenneth Anderson, *Targeted Killing in U.S. Counterterrorism Strategy and Law* (May 11, 2009), *available at* http://opiniojuris.org/2009/06/06/targeted-killing-in-us-counterterrorism-strategy-and-law/.

46. *See* Ward Carr, *Surviving the Bismarck's Sinking*, 20 NAVAL HISTORY 54 (2006).

47. *See* EDWARD PAICE, WORLD WAR I: THE AFRICAN FRONT: AN IMPERIAL WAR ON THE DARK CONTINENT 1–3 (2008).

ritory of a neighboring State based on the threat dynamics, they have always done so.[48]

History demonstrates that the scope of armed conflict—whether international or non–international—is threat driven. Strategic reality indicates that States engaged in armed conflict will, and in fact often must, "take the fight to the enemy." But this does not mean that other considerations, principally diplomatic and political, are not also relevant to the actual scope of military operations associated with an armed conflict. Like so many other aspects of international law, authority rarely imposes obligation, and States take into account a variety of diplomatic, military and policy considerations when choosing when and where to assert combat power against an enemy. One element in this equation is always the tactical, operational and strategic value of attacking a particular lawful target. This value assessment must be balanced against second and third–order negative consequences of exercising attack authority. In the "hot zone" context, this analysis is central to the tactical and operational targeting process, where commanders routinely refrain from attacking a lawful target because they conclude doing so will not be worth the costs attendant in attack.[49] At the strategic level, when the target is identified outside the "hot zone," diplomatic consequences of asserting military power in the territory of another State must be included among these "costs." Because such costs are so significant, States often refrain from exercising this authority.

In the international armed conflict context, the law of neutrality provides an effective framework for assessing when such military action is lawful.[50] Neutrality law also provides belligerent States with the legal leverage to demand neutral States refrain from conduct that would trigger the need for such military action.[51] Unfortunately, the principles established by the law of neutrality are inapposite to TAC. Indeed, TAC is in many ways *sui generis*, as it involves a military response to highly dispersed enemy capabilities and fleeting windows of opportunity to target those capabilities. Thus, the value of attacking such targets in TAC has obviously been perceived as

48. Vité, *supra* note 4.

49. International Security Assistance Force–Kabul, Afghanistan, Tactical Directive (July 6, 2009), *available at* http://www.nato.int/isaf/docu/official_texts/Tactical_Directive_090706.pdf; Marybeth P. Ulrich, *The General Stanley McChrystal Affair: A Case Study in Civil-Military Relations*, 41 PARAMETERS: U.S. ARMY WAR COLLEGE 86, 93 (2011) (discussing General McChrystal's decision to limit attack authority).

50. *The Law of Armed Conflict Neutrality*, *supra* note 21.

51. *Id.*

far more significant than attacking enemy targets outside "hot zones" of conflict in the context of more conventional inter–State or intra–State armed conflicts.

Consequently, the geographic scope of operations associated with TAC presents unique challenges (if not dilemmas). Unlike the accepted typology of international conflicts—inter–State armed hostilities—the geographic scope of TAC is not framed by the complementary international legal principles of neutrality. However, unlike the accepted non–international conflict typology—internal armed hostilities—the enemy center of gravity and/or attacks that will produce decisive effect will often be located in areas far removed from "hot zones". Understanding this dynamic is critical to assessing the validity or wisdom of imposing a geographic "box" on permissible TAC scope. Operational range is not an arbitrary element of LOAC regulation. It is, instead, a logical consequence of the nature of the conflicts themselves: in the more conventional context—be it international or non–international armed conflict—the enemy center of gravity is rarely dispersed beyond the hot zone of conflict. In contrast, the enemy in TAC deliberately avoids consolidating its center of gravity in such zones, but instead operates out of whatever safe haven offers the best opportunity for protection from the reach of State military capabilities.[52]

This does not mean that the uncertainties created by the intersection of threat–based scope and TAC are insignificant. To the contrary, extending the concept of armed conflict to a transnational non–State opponent has resulted in significant discomfort related to the assertion of State military power. But attempting to decouple the permissible geography of armed conflict from threat–driven strategy by imposing some arbitrary legal limit on the geographic scope of TAC is an unrealistic and ultimately futile endeavor. Other solutions to these uncertainties must be pursued—solutions that mitigate the perceived overbreadth of authority associated with TAC. As explained below, these solutions should focus on four considerations:

(1) managing application of the inherent right of self–defense when it results in action within the sovereign territory of a non–consenting State;
(2) adjusting the traditional targeting methodology to account for the increased uncertainties associated with TAC threat identification;

52. *See* National Security Strategy, *supra* note 25.

(3) considering the feasibility of a "functional *hors de combat*" test to account for incapacitating enemy belligerents incapable of offering hostile resistance; and
(4) continuing to enhance the process for ensuring that preventive detention of captured belligerent operatives does not become unjustifiably protracted in duration.

This essay does not seek to develop each of these mitigation measures in depth. Instead, it proposes that focusing on these (and perhaps other innovations in existing legal norms) is a more rational approach to mitigating the impact of TAC than imposing an arbitrary geographic scope limitation. Other scholars have already begun to examine some of these concepts, a process that will undoubtedly continue in the future. Whether these innovations take the form of law or policy is another complex question, which should be the focus of exploration and debate. In short, rejecting the search for geographic limits on the scope of TAC should not be equated with ignorance of the risks attendant with this broad conception of armed conflict. Instead, it must be based on the premise that even if such a limit were proposed, it would ultimately prove ineffective in preventing the conduct of operations against transnational non–State threats where the State concludes such operations will produce a decisive effect. Instead, focusing on the underlying issues themselves and considering how the law might be adjusted to account for actual or perceived authority overbreadth is a more pragmatic response to these concerns.

A. Jus ad Bellum *and the Authority to Take the Fight to the Enemy*

One example of proposals to mitigate the risk of overbreadth associated with TAC is the "unable or unwilling" test highlighted by the scholarship of Professor Ashley Deeks.[53] Deeks proposes a methodology for balancing a State's inherent right to defend itself against transnational non–State threats and the sovereignty of other States where threat operatives are located. Because the law of neutrality cannot provide the framework for balancing these interests (as it does in the context of international armed conflicts), Deeks acknowledges that some other framework is necessary to limit resort to military force outside "hot zones," even when justified as a measure of national self–defense. The test she proposes seeks to limit self–

53. *See* Deeks, *supra* note 18.

help uses of military force to situations of absolute necessity by imposing a set of conditions that must be satisfied to provide some objective assurance that the intrusion into another State's territory is a genuine measure of last resort.[54] This is pure *lex lata*,[55] so is Deeks, to an extent. However, Deeks, having served in the Department of State Legal Advisor's Office, recognizes that *if* TAC is a reality (which it is for the United States), these innovations are necessary to ensure it does not result in unjustifiably overbroad U.S. military action.

B. Target Identification and Engagement

This is precisely the approach that should be considered in the *jus in bello* branch of conflict regulation to achieve an analogous balance between necessity and risk during the execution of combat operations. Even assuming the "unable or unwilling" test effectively limits the exercise of national self–defense in response to transnational terrorism, it in no way mitigates the risks associated with the application of combat power once an operation is authorized.

The *in bello* targeting framework is an obvious starting point for this type of exploration of the concept and its potential adjustment.[56] Indeed, it seems increasingly apparent that while TAC suggests a broad scope of authority to employ combat power in a LOAC framework with no geographic constraint, the consternation generated by this effect is a result of the uncertainty produced by the complexity of threat recognition. This consternation is most acute in relation to three aspects of action to incapacitate terrorist belligerent operatives: the relationship between threat recognition and the authority to kill as a measure of first resort (the difficulty of applying the principle of distinction when confronting irregular enemy belligerent forces); the pragmatic illogic of asserting the right to kill as a measure of first resort to an individual subject to capture with virtually no risk to U.S. forces; and the ability to apply this targeting authority against unconventional enemy operatives located outside of "hot zones".[57]

---

54. *See id.* at 507–8.

55. J. Jeremy Marsh, *Lex Lata or Lex Ferenda? Rule 45 of the ICRC Study on Customary International Humanitarian Law*, 198 MILITARY LAW REVIEW 116, 121–25 (2008).

56. *See* YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT (4th ed. 2004); Corn & Jensen, *supra* note 16.

57. *See* Reply Memorandum in Support of Plaintiff's Motion for a Preliminary Injunction and in Opposition to Defendants' Motion to Dismiss, *Al-Aulaqi v. Obama*, 727 F.

These concerns flow from the intersection of a battlespace that is functionally unrestricted by geography and the unconventional nature of the terrorist belligerent operative. The combined effect of these factors is a target identification paradigm that defies traditional threat recognition methodologies: no uniform, no established doctrine, no consistent locus of operations and dispersed capabilities.[58] It is certainly true that threat identification challenges are in no way unique to TAC; threat identification has always been difficult, especially in the context of "traditional" non–international armed conflicts involving unconventional belligerent opponents. Yet, when this threat recognition uncertainty was confined to the geography of one State, it was never perceived to be as problematic as it is in the context of TAC. This is perplexing. In both contexts, the unconventional nature of the enemy increases the risk of mistake in the target selection and engagement process.[59] Thus, employing the same approach is completely logical.

Two factors appear to provide an explanation for the increased concern over the threat identification uncertainty in the context of TAC. One of these is beyond the scope of "mitigation solutions," while the other is not. The first is the increased public awareness and interest in both the legal authority to use military force and the legality of the conduct of hostilities, a factor that inevitably increases the scrutiny on military power under the rubric of TAC. This pervasive and intense interest in and legal critique of military operations associated with what is euphemistically called the war on terror is truly unprecedented. In this "lawfare" environment, it is unsurprising that government action that deprives individuals of life as a measure of first resort or subjects them to preventive detention that may last a lifetime—often impacting individuals located far beyond a "hot zone" of armed hostilities—generates intense legal scrutiny.[60] This factor, whether a

---

Supp. 2d 1 (D.D.C. 2010) (No. 10-cv-01469); Daskal*, supra* note 17; *Pakistan Unrelenting in Demanding Drone Strike End*, CBS NEWS (July 30, 2012), http://www.cbsnews.com/8301-501363_162-57482623/pakistan-unrelenting-in-demanding-drone-strike-end/.

58. *See* Geoffrey S. Corn & Gary P. Corn, *The Law of Operational Targeting: Viewing the LOAC Through an Operational Lens*, 47 TEXAS INTERNATIONAL LAW JOURNAL 337 (2012) [hereinafter Corn & Corn]; Geoffrey S. Corn, *Targeting, Command Judgment, and a Proposed Quantum of Information Component*, 77 BROOKLYN LAW REVIEW 437 (2012).

59. Corn, *supra* note 7.

60. The ACLU drone litigation is the first lawsuit in modern history challenging legal authority for wartime targeting. *See* ACLU v. DOJ, No. 10-436, 2011 WL 4005324 (D.D.C. Sept. 9, 2011).

net positive or negative, is a reality that is unlikely to abate in the foreseeable future.

The second factor—a factor that is amenable to adjustments in legal authorities to ameliorate the perceived overbreadth of TAC—is the perception that this risk of targeting error when attacking unconventional forces increases proportionally with the attenuation from a "hot zone" of operations.[61] Whether there is any empirical foundation for this perception is uncertain, nor is it clear that the assumption itself is valid. However, in many ways perception has become reality.

In an article published in the *Brooklyn Law Review*, I proposed a sliding quantum of information related to the assessment of targeting legality based on relative proximity to a "hot zone."[62] In essence, I proposed that when conducting operations against unconventional non–State operatives, the reasonableness of a target legality judgment requires increased informational certainty the more attenuated the nominated target becomes to a zone of traditional combat operations. The concept was proposed as a measure to mitigate the increased risk of targeting error when engaging an unconventional belligerent operative in an area that itself does not indicate belligerent activity. Jennifer Daskal offers a similar proposal in her article, *The Geography of the Battlefield*.[63] Daskal presents a more comprehensive approach to adjusting the traditional targeting framework when applied to the TAC context. Both of these articles seek to mitigate the consequence of applying broad LOAC authority against a dispersed and unconventional enemy; both methods that should continue to be explored.

C. The Capture or Kill Dilemma?

One of the issues Daskal addresses in her article beyond that of target identification is the legitimacy of applying the authority to kill as a measure of first resort to enemy belligerents outside "hot zones" of hostilities.[64] This issue is obviously a focal point of the contemporary debate over the use of unmanned aerial systems (armed drones) to attack belligerent operatives. It

---

61. This is the foundation for Daskal's hot zone article. *See* Daskal, *supra* note 17.

62. *Targeting, Command Judgment, and a Proposed Quantum of Information Component*, *supra* note 58, at 460–94 ("The greater the presumption that a potential object of attack is not a legal military objective, the greater the quantum of information necessary to justify attacking the target.").

63. *See* Daskal, *supra* note 17.

64. *Id.*

is also at the center of the debate related to the authority to engage civilians taking a direct part in hostilities.[65] What Daskal proposes, which is analogous to the ICRC *DPH Interpretive Guidance*,[66] is that capture (rather than kill) should be obligatory when it is a feasible alternative to employing deadly force.[67]

No single aspect of the *DPH Interpretive Guidance* generated more controversy than Section IX of the study, which asserted an identical obligation to capture instead of kill civilians engaged in DPH whenever feasible.[68] In support of this assertion, the study relies on an article published by Jean Pictet (the well–known author of the ICRC commentaries to the 1949 Geneva Conventions) in which he asserts that the principle of humanity obligates belligerents to refrain from using deadly force against enemy belligerents when capture is a "risk free" alternative.[69] Many LOAC experts, including this author, contest this interpretation of the law, arguing instead

---

65. NILS MELZER, INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW (May 2009) (prepared by Nils Melzer) [hereinafter ICRC DPH Interpretive Guidance], *available at* http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf ("[T]he kind and degree of force which is permissible against persons not entitled to protection against direct attack must not exceed what is actually necessary to accomplish a legitimate military purpose in the prevailing circumstances."); *see* W. Hays Parks, *Part IX of the ICRC "Direct Participation in Hostilities" Study: No Mandate, No Expertise, and Legally Incorrect*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 769 (2010) (responding to the new guidance).

66. ICRC DPH Interpretative Guidance, *supra* note 65.

67. *See* Daskal, *supra* note 17.

68. *See* ICRC DPH Interpretive Guidance, *supra* note 65.

69. As found in Parks, *supra* note 65, at 785–87. According to footnote 221 of the *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*,

> It is in this sense that Pictet's famous statement should be understood that "[i]f we can put a soldier out of action by capturing him, we should not wound him; if we can obtain the same result by wounding him, we must not kill him. If there are two means to achieve the same military advantage, we must choose the one which causes the lesser evil". See Pictet, Development and Principles of International Humanitarian Law (Dordrecht, Nijhoff 1985), pp. 75 f. During the expert meetings, it was generally recognized that the approach proposed by Pictet is unlikely to be operable in classic battlefield situations involving large-scale confrontations (Report DPH 2006, pp. 75 f., 78) and that armed forces operating in situations of armed conflict, even if equipped with sophisticated weaponry and means of observation, may not always have the means or the opportunity to capture rather than kill (Report DPH 2006, p. 63).

See ICRC DPH Interpretive Guidance, *supra* note 65, at 82 n.221.

that unless and until the enemy belligerent becomes *hors de combat*, the law permits the application of deadly force as a measure of first resort.[70]

There is, however, a common thread that runs through the ICRC *DPH Interpretive Guidance*, precursors to the *Interpretive Guidance* (most significantly the Israeli High Court of Justice decision on targeted killings),[71] Daskal's proposal, and Pictet's interpretation of the principle of humanity: the obvious discomfort with a legal norm that permits the killing of a human being when capture provides a risk–free alternative for achieving the goal of incapacitation. In my article *Mixing Apples and Hand Grenades*,[72] I attempt to explain why this apparent overbreadth of deadly force authority is an unfortunate yet necessary aspect of armed hostilities, and I remain unpersuaded that the law imposes an implicit limitation of the authority to use deadly force based on the unconventional nature of the belligerent opponent or the opponent's geographic location.

While a capture–instead–of–kill obligation remains a controversial assertion, what is undisputed is that LOAC prohibits deliberate attacks on any person not actively participating in hostilities, whether a civilian who has directly participated in hostilities or a belligerent who is *hors de combat*. Traditionally, an enemy belligerent is rendered *hors de combat* only as the result of wounds, sickness or surrender. The normal application of this LOAC principle permits attack on enemy belligerent operatives—members of organized belligerent groups engaged in hostilities—regardless of their location, or the ease with which they might be captured, so long as they are still "combat effective," even when they pose no immediate or apparent threat.[73] This seemingly harsh outcome is justified by a number of considerations. It is ultimately based on the presumption that a fully functional member of an enemy belligerent group represents an ongoing threat, and attacking that individual is linked to bringing about the submission of the group writ large.[74]

This explains why many LOAC experts reject the suggestion that an enemy belligerent operative is somehow immune from attack as the result

---

70. ICRC DPH Interpretive Guidance, *supra* note 65; Geoffrey S. Corn, *Mixing Apples and Hand Grenades: The Logical Limits of Applying Human Rights Norms to Armed Conflict*, 1 JOURNAL OF INTERNATIONAL HUMANITARIAN LEGAL STUDIES 52 (2010).

71. *See* Parks, *supra* note 65, at 788–93.

72. *See Mixing Apples and Hand Grenades, supra* note 70.

73. *See* Gabriella Blum, *The Dispensable Lives of Soldiers*, 2 JOURNAL OF LEGAL ANALYSIS 115 (2010) (noting how the harshness of this rule has led some to question its continuing validity) [hereinafter Blum].

74. *See Mixing Apples and Hand Grenades*, *supra* note 70; Parks, *supra* note 65.

of being in a location where he can be safely captured. However, the combined effect of being in such a location—especially a location distant from any ongoing active combat operations—with the conclusion that the operative is unarmed and functionally inoffensive (for example, an unarmed al Qaeda operative exiting a commercial airliner at a U.S. airport while under close observation by government agents) explains why this assertion of kill authority is criticized as unjustifiably over–broad.

The debate is symbolic of the overall challenge to the current response to transnational terrorism through the armed conflict modality: it reveals an effort to push a square peg into a round hole. It is clear that the "kill authority" analytical methodology is derived from a predominantly conventional conflict context. In that context, the balance of interests justifies the at times over–broad application of deadly combat power, and altering this equation produces an unjustified shift of risk to attacking forces (a point I attempted to explain in *Mixing Apples and Hand Grenades*).[75] Perhaps, however, the context of geographically dispersed combat operations within the framework of TAC warrants consideration of imposing a policy–based constraint on this authority, what might be characterized as a functional *hors de combat* test. Such a test would limit "kill authority" when tactical assessment indicates that capture is completely feasible without subjecting friendly forces to risk, and the object of capture is attenuated from *both* an area of active combat operations and other belligerent operatives.

Ironically, when Professor Gabrielle Blum proposed such a limitation in her article *The Dispensable Lives of Soldiers*,[76] I was quite skeptical. However, my skepticism focused primarily on two considerations. First, her proposal extended to "hot zones". I remain opposed to such an extension, as I believe it would inject a dangerous dilution of tactical initiative into the execution of combat operations.[77] Second, it was unclear whether Professor Blum was proposing a legal norm, or a policy constraint on permissible legal authority. Once it was clear that we shared opposition to modifying the existing legal authority to attack even an inoffensive enemy belligerent operative (such as an enemy soldier sleeping in a barracks or assembly area or attempting to retreat from an ongoing attack), and that she was in fact

75. *Mixing Apples and Hand Grenades*, *supra* note 70, at 84–90.
76. Blum, *supra* note 73.
77. *See Mixing Apples and Hand Grenades*, *supra* note 70.

proposing consideration of policy limits on that authority, we were much more closely aligned in our views.[78]

This latter aspect of the "capture or kill" debate is critical, and in my opinion, if such a limitation on targeting authority is justified, it must be framed as a policy limit on otherwise lawful authority: a rule of engagement.[79] This is because there may be situations, even where these conditions are satisfied, when an attack is justified because of the influence it will produce on enemy leadership and other belligerent operatives. It is this corporate, as opposed to individualized, approach to attack justification that distinguishes targeting belligerent operatives from targeting civilians taking a direct part in hostilities. It therefore requires strictly limiting any "capture or kill" obligation to a policy applique restricting underlying legal authority. In short, even when capture is a completely feasible option to incapacitate an enemy belligerent operative, there still are times when attack is preferred because of the shock effect it will produce on the corporate enemy capability.[80]

Such a policy may also be a useful method to alleviate the uncertainties associated with the intersection of belligerent detention authority and belligerent targeting authority. The complexity of this connection seems to have been highlighted by Justice Kennedy early in our TAC with al Qaeda, when he challenged the government to articulate a unified theory of detention/attack authority in the *Padilla* oral arguments.[81] In response to the government's assertion that Padilla's status as an enemy belligerent justified his LOAC–based preventive detention, Justice Kennedy asked a question that the government never answered: would that same status justify killing Padilla as he walked off the plane at Chicago O'Hare Airport?

> QUESTION: Would you shoot him when he got off the plane?
>
> MR. CLEMENT: No, I don't think we could for good and sufficient reasons –

78. Gabriella Blum, Address Before the American Society of International Law, Mind the Gap: International Human Rights Law and the Law of Armed Conflict (Jan. 25, 2010), audio recording available at http://www.asil.org/files/100125mindthegap.mp3.

79. *See* Corn & Corn, *supra* note 58, at 353–57.

80. *Mixing Apples and Hand Grenades*, *supra* note 70, at 80 ("attacking the enemy with deadly combat power is customarily considered necessary to force an opponent into submission.")

81. Transcript of Oral Argument at 21, Rumsfeld v. Padilla, 542 U.S. 426 (2004) (No. 03-1027).

> QUESTION: I assume that you could shoot someone that you had captured on the field of battle.[82]

The Solicitor General offered a false analogy in response to this question, asserting that once an individual is *captured* the authority to kill dissipates. This is simply an application of the *hors de combat* rule, and is unremarkable. However, what the question really exposed was whether the authority to kill—an authority triggered by enemy belligerent status—applied *prior* to capture where capture was a completely feasible course of action. That question remains relevant, and by subjecting kill authority to a policy–based constraint it will perhaps strike a more effective balance between necessity and humanity and contribute to a logical synchronization between the exercise of detention and targeting authority for individuals captured in situations similar to those of Padilla. (Interestingly, the Solicitor General ultimately relied on rules of engagement to complete his response to the question: "And I think in every case, there are rules of engagement, there are rules for the appropriate force that should be used. And I don't know that there are any.")[83]

This "functional *hors de combat*" concept and accordant policy limitation on the use of deadly force as a first resort is something I have only begun to consider. However, it seems clear that addressing the perceived overbreadth of "kill authority" within the context of TAC is an important endeavor that may effectively respond to arguments claiming that the TAC concept is illegitimate. Developing a rational methodology to assess when the kill option is justified, or when capture should be attempted as a condition precedent—even if only in the form of policy—would be a potentially valuable advancement in the complex equation of unconventional enemy belligerent targeting.

D. Long–Term Preventive Detention

Capture, of course, produces its own complex issues of perceived ovebreadth, all flowing from subjecting captives to LOAC–based preventive detention. Debates over the legitimacy of designating terrorist operatives as enemy belligerents and subjecting them to LOAC detention principles has raged since the first detainees were transferred to Guantanamo

82. *Id.*
83. *Id.*

Bay, Cuba, in 2001.[84] While far from a consensus view, for the purposes of U.S. practice, this legitimacy issue has been resolved in favor of the authority to detain individuals based on a determination of status as an enemy belligerent (although how that determination is made, both substantively and procedurally, is an area of U.S. practice that continues to evolve).[85] Detention review procedures have been another source of controversy, and have developed substantially since the inception of the belligerent detentions.[86] As long as debates continue in full force over the credibility of the procedures adopted for assessing or revalidating enemy belligerent classifications and the judicial review of these decisions, it is unlikely these current procedures will undergo further substantial modification. Instead, it seems relatively clear that the government has reached the point where it believes these procedures are both operationally effective and legally defensible—an inference bolstered by the overall record of government success in the D.C. Circuit Court of Appeals. Two issues, however, should be subjected to more intense development: who should represent detainees in the status determination process, and how to determine when preventive detention should terminate.

From the inception of the unprivileged detention operation, the United States has chosen not to provide suspected enemy belligerents with assistance of legal counsel.[87] Instead, the review process implemented to assess this status—both at Guantanamo and in Afghanistan—has relied on lay military officers to assist detainees through the proceedings.[88] This practice is apparently the result of analogy to the process established in Article 5 of

84. Chris Jenks & Eric T. Jensen, *Indefinite Detention Under the Laws of War*, 22 STANFORD LAW AND POLICY REVIEW 41, 51–55 (2011) ("[T]he deconstructionist approach removes a large portion of internationally recognized and accepted provisions for regulating detention associated with armed conflict—the Geneva Conventions—while leaving the underlying question of how to govern detention unanswered.")

85. *Id.*

86. *See* 28 U.S.C. § 2241 (2012); Boumediene v. Bush, 553 U.S. 723 (2008); Hamdi v. Rumsfeld, 542 U.S. 507 (2004); Exec. Order No. 13,567, 76 Fed. Reg. 13277 (Mar. 7, 2011); Jeff A. Bovarnick, *Detainee Review Boards in Afghanistan: From Strategic Liability to Legitimacy*, THE ARMY LAWYER (DA PAM 27-50-445) (June 2010).

87. Jenny S. Martinez, *Process and Substance in the "War on Terror,"* 108 COLUMBIA LAW REVIEW 1013, 1037–38 ("[T]he legality of... military detention and interrogation without access to counsel remains unresolved.").

88. *See* memorandum from Paul Wolfowitz, Deputy Secretary of Def., Order Establishing Combatant Status Review Tribunal (July 7, 2004), *available at* http://www.defenselink.mil/news/Jul2004/d20040707review.pdf.

the Third Geneva Convention for resolving doubt as to whether captives qualify for prisoner of war status.[89]

In a recently published article, *Unprivileged Belligerents*,[90] I challenge the underlying rationale for this lay assistance model. Specifically, I argue that the stakes involved in these review proceedings and the inherent complexity of granting status to non–State belligerent actors—a difficulty caused by the need to rely on pre–capture conduct and affiliation as opposed to the much easier reliance on uniform or other formal belligerent identification indicators—justifies assistance of legal officers. While I acknowledge that lay officers are certainly capable of learning the procedures applicable to these review proceedings, I question whether non–lawyers can effectively represent the interests of suspected enemy operatives. In contrast, I assert that the ethos of zealous representation—a core ethical norm of the legal profession—will enhance the quality and legitimacy of the detainee–status–determination process.

This lay–representation paradigm has finally been called into question. The extremely controversial provisions of the National Defense Authorization Act for Fiscal Year 2012, authorizing preventive military detention of U.S. and alien terrorist operatives, include, for the first time, a mandate to provide detainees with legal representation during detention review proceedings.[91] The statute, signed into law by President Obama on December 19, 2011, provides that the Secretary of Defense must submit to Congress within ninety days of enactment a report "setting forth the procedures for determining the status of persons captured in the course of hostilities authorized by the Authorization for Use of Military Force (Public Law 107–40) for purposes of section 1021."[92] The law then provides, *inter alia*, that

89. Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 1355, art. 5 [hereinafter Geneva Convention III].

90. Geoffrey S. Corn & Peter A. Chickris, *Unprivileged Belligerents, Preventive Detention, and Fundamental Fairness: Rethinking the Review Tribunal Representation Model*, SANTA CLARA JOURNAL OF INTERNATIONAL LAW 115 (2012).

91. National Defense Authorization Act for Fiscal Year 2012, Public Law No. 112-81 § 1024(a), 125 Stat. 1298, 1565 (2011).

92. Section 1021 "affirms that the authority of the President to use all necessary and appropriate force pursuant to the Authorization for Use of Military Force . . . includes the authority. . . to detain covered persons. . . pending disposition under the law of war." *Id.* § 1021(a). Persons who may be detained under section 1021 include persons "who planned, authorized, committed, or aided . . . or harbored those responsible" for the attacks occurring on September 11, 2001 as well as persons who were

"an unprivileged enemy belligerent may, at the election of the belligerent, be represented by military counsel at proceedings for the determination of status of the belligerent."[93]

It is not yet clear at what point in the detention process this assistance of counsel requirement will become operative. According to the Conference Report on the NDAA:

> The Senate amendment contained a provision (sec. 1036) that would require the Secretary of Defense to establish procedures for determining the status of persons captured in the course of hostilities authorized by the Authorization for Use of Military Force (Public Law 107–40), including access to a military judge and a military lawyer for an enemy belligerent who will be held in long–term detention. The House bill contained no similar provision.
>
> The House recedes with an amendment clarifying that the Secretary of Defense is not required to apply the procedures for long–term detention in the case of a person for whom habeas corpus review is available in federal court. Because this provision is prospective, the Secretary of Defense is authorized to determine the extent, if any, to which such procedures will be applied to detainees for whom status determinations have already been made prior to the date of the enactment of this Act. The conferees expect that the procedures issued by the Secretary of Defense will define what constitutes "long–term" detention for the purposes of subsection (b). The conferees understand that under current Department of Defense practice in Afghanistan, a detainee goes before a Detention Review Board for a status determination 60 days after capture, and again 6 months after that. The Department of Defense has considered extending the period of time before a second review is required. The conferees expect that the procedures required by subsection (b) would not be triggered by the first review, but could be triggered by the second review, in the discretion of the Secretary.[94]

Thus, legal representation will now turn on the definition of "long–term" detention. Nonetheless, this is an important step forward in the procedural

---

> a part of or substantially supported al–Qaeda, the Taliban, or associated forces that are engaged in hostilities against the United States or its coalition partners, including any person who has committed a belligerent act or has directly supported such hostilities in aid of such enemy forces.

Id. § 1021(b).

93. *Id.* § 1024(b)(2).

94. H.R. REP. NO. 112-329, pt. 1, at 696–97 (2011).

protections afforded individuals subjected to wartime preventive detention. Whatever emerges as the ultimate triggering point, the detention review process will undoubtedly be enhanced by this provision. While no amount of process will ameliorate the concerns of critics of the fundamental concept of applying wartime preventive detention to counterterror operations, even the most ardent of such critics must acknowledge that providing representatives trained in the lawyer ethos of zealous representation is a marked improvement to the lay representation model utilized prior to the enactment of the NDAA 2012.

Preventive detention based on a determination of belligerent status, like targeting based on the same categorization, is central to the entire TAC concept. The ability to use combat power to kill as a measure of first resort compared to detention that prevents a return to belligerent activities are the two most significant authorities triggered by the armed conflict characterization. It is therefore unlikely that the United States will abandon this detention regime, which, as the U.S. Supreme Court noted in *Boumediene v. Bush*, may continue for an entire generation.[95] When the stakes of a factual determination by a review tribunal—even one not related to punitive sanction—are so obviously profound, it is fair to ask whether reliance on lay military officers to represent the interests of alleged belligerent operatives can genuinely be considered legitimate. If legitimacy is defined by a credible and fair balance between the interests of protecting national security and the interests inherent in safeguards from arbitrary detention, it seems difficult to ignore the potential value legal assistance might add to the accuracy of the belligerent status determination.

Once that decision is made, with or without assistance of counsel, the impact is clear: preventive detention for the duration of hostilities. But this raises an even more complex and in many ways troubling incongruity between the nature of the ongoing TAC against al Qaeda and the LOAC principles upon which this detention model is based: when should detention terminate? This question is critically important to the credibility and legitimacy of asserting LOAC authority to justify detention. The entire unprivileged belligerent detention regime is built on the premise that detention is justified for the duration of hostilities to prevent the belligerent

95. *See generally* Boumediene v. Bush, 553 U.S. 723 (2008) (extending the constitutional writ of habeas corpus to unprivileged enemy belligerents detained at Guantanamo Naval Base based on the conclusion, *inter alia,* that "the consequence of error may be detention of persons for the duration of hostilities that may last a generation or more, the risk too significant to ignore.").

from returning to operations.[96] This principle derives from LOAC and, in the context of more conventional armed conflicts, is virtually axiomatic.[97] However, it seems equally clear that the principle of incapacitation by detention for the duration of hostilities was not developed in contemplation of an armed conflict of unlimited duration. This aspect of the current detention regime is exacerbated by the nature of the armed conflict, in which some type of formal or explicit recognition of hostility termination by the belligerent parties is virtually inconceivable (this is certainly not the case in the context of inter–State hostilities, or even intra–State hostilities involving organized armed groups).[98]

It is therefore unsurprising that one of the most consistent criticisms of U.S. detention policy has been that it authorizes indefinite detention.[99] This is virtually inconceivable in any other context, regardless of whether the individual is detained within a punitive or preventive framework. One solution to this issue, of course, is to abandon LOAC–based preventive detention entirely. This, however, is unlikely in the foreseeable future, which leads some scholars to critique the potential overbreadth of purely status–based preventive detention—even within a LOAC framework. For example, in their article, *Indefinite Detention Under the Laws of War*,[100] Professors (and retired military lawyers) Jenks and Jensen assert that what might be best understood as "conduct–based detention validation" procedures extrapolated from LOAC civilian internment rules would effectively address the risk of unjustified indefinite detention of unprivileged enemy belligerents.[101]

An alternate modification is the imposition of presumptive detention termination dates linked to adjusted burdens that justify continued deten-

96. Hamdi v. Rumsfeld, 542 U.S. 507, 518 (2004) ("We conclude that detention of individuals falling into the limited category we are considering, for the duration of the particular conflict in which they were captured, is so fundamental and accepted an incident to war as to be an exercise of the necessary and appropriate force Congress has authorized the President to use.") (internal quotations omitted).

97. *See* Geneva Convention III, *supra* note 89.

98. List of Recent Peace Agreements, U.S. INSTITUTE FOR PEACE, http://www.usip.org/publicationstools/latest?filter1=**ALL**&filter0=**ALL**&filter2=2223&filter3=**ALL**&filter4=%20(last%20visited%20Aug.%2014,%202012).

99. *See* Laurie R. Blank, *Square Peg in a Round Hole: Stretching Law of War Detention Too Far*, 63 RUTGERS LAW REVIEW 1169, 1183–91 (2011) (noting the "inherently punitive" nature of holding suspected terrorists indefinitely under the guise of prisoners of war).

100. *See* Jenks & Jensen, *supra* note 84.

101. *Id.* at 87–91 (addressing the various ways detention is authorized to end according to LOAC principles).

tion. Drawing an analogy to procedures for declassification of national security information, this approach would begin by assessing the extreme end state for prisoners of war detentions since 1949. Such an assessment suggests that almost all such detentions terminated within ten years from inception.[102] Thus, for example, a policy might be adopted that would create a presumptive detention termination date ten years from the date of inception. Like the declassification context, this presumption would not be conclusive. Instead, it would impose on the government a rebuttable burden to justify continuing preventive detention beyond—or even until—presumptive termination. Subsequent duration triggers could be adopted that would increase the burden of proof on the government, leading ultimately to a requirement that the government must justify what would be in effect "generational" detention by proving beyond a reasonable doubt that the detainee is likely to return to belligerent activities.

Perhaps neither of these approaches is ideal, but both share the common goal of aligning long–term preventive detention—what is in effect indefinite detention—with a legitimate determination of necessity. Like the other adjustments suggested by this essay, accomplishing this goal will mitigate the actual and perceived overbreadth of asserting LOAC authority within a TAC framework.

Perhaps other modifications to existing LOAC authorities should also be explored to achieve this objective. Devoting academic and policy efforts toward these and other similar authority adjustments will produce a more positive effect than fishing for the *Red Herring* of a defined geography of armed conflict. This is precisely because they will be rooted in both operational logic and humanitarian considerations, thereby increasing the likelihood of being accepted as consistent with strategic imperatives—not as an arbitrary legal fiction inconsistent with a threat–driven strategic reality.

IV. CONCLUSION

The law of conflict regulation is arguably at a critical crossroads. If threat drives strategy, and strategy drives the existence of armed conflict, the concept of TAC seems an unavoidable reality in the modern strategic envi-

102. *See* Piero Scaruffi, *Wars and Genocides of the 20th Century*, Scaruffi.com, http://www.scaruffi.com/politics/massacre.html (last visited Aug. 14, 2012); *see also* SUSANNE EVERETT, WARS OF THE 20TH CENTURY (1986). *See generally List of Wars 1945–1989*, WIKIPEDIA, http://en.wikipedia.org/wiki/List_of_wars_1945–1989 (last visited Aug. 14, 2012).

ronment. Opponents of TAC will continue to argue for limiting armed conflict to the well–accepted inter–State or intra–State hostilities frameworks, but this would only drive States to adopt *sub rosa* uses of the same type of power under the guise of legal fictions. Concepts such as self–defense targeting, or internationalized law enforcement, might avoid the armed conflict characterization, but they would do little to resolve the underlying uncertainties associated with TAC. Even worse, they would inject regulatory uncertainty into the planning and execution of military counterterror operations, and expose those called upon to put themselves in harm's way to protect the State to legal liabilities based on inapposite legal norms.

If, however, the geographic scope of TAC is accepted as a threat–driven dynamic, then it seems imperative to consider how the law will respond to the uncertainties created by this reality and addressed in this essay. What conduct results in the designation of belligerent status? Should there be an individualized, "imminence" assessment associated with targeting suspected belligerent operatives outside a "hot zone" of conflict? How certain must an operational commander be before reaching this conclusion? Should capture instead of kill be a legal or policy obligation outside the "hot zone?" Should there be a presumptive termination date for belligerent detention authority, requiring the State to justify continued detention by some burden sufficiently weighty to protect individuals from *arbitrary* indefinite detention?

These are all important and legitimate questions that should be the focus of legal debate and analysis. TAC may provide a framework based on core LOAC principles within which to assess these questions, but TAC in no way conclusively resolves them. Instead, it was originally conceived as a typology of armed conflict that reconciled the denial of privileged belligerent legitimacy for the terrorist enemy with the obligation to respect fundamental LOAC norms in the execution of such operations (to include the detention and treatment of captured terrorist belligerents), all within the strategic imperative of robust global counterterror operations. No other typology fully satisfied these goals—goals that drove the U.S. response to September 11. The lingering questions associated with this effort to synchronize strategic objectives with legal regulation must be the focal point of critical analysis regarding the future of irregular warfare.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions

Matthew C. Waxman

89 INT'L L. STUD. 109 (2013)

Volume 89 2013

Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions

Matthew C. Waxman[*]

I. INTRODUCTION

When does a cyber attack (or threat of cyber attack) give rise to a right of self-defense—including armed self-defense—and when should it? By "cyber attack" I mean the use of malicious computer code or electronic signals to alter, disrupt, degrade or destroy computer systems or networks or the information or programs on them. It is widely believed that sophisticated cyber attacks could cause massive harm—whether to military capabilities, economic and financial systems, or social functioning—because of modern reliance on system interconnectivity, though it is highly contested how vulnerable the United States and its allies are to such attacks.[1]

* Professor, Columbia Law School; Adjunct Senior Fellow, Council on Foreign Relations; Member of the Hoover Institution Task Force on National Security and Law.

1. *See* Mark Clayton, *The New Cyber Arms Race*, CHRISTIAN SCIENCE MONITOR (Mar. 7, 2011), http://www.csmonitor.com/USA/Military/2011/0307/The-new-cyber-arms-race. Some experts warn of a "digital Pearl Harbor" or other likely devastating attacks on the United States. *See*, *e.g.*, Mike McConnell, *To Win the Cyber-War, Look to the Cold War*, WASHINGTON POST, Feb. 28, 2010, at B1. Other experts, however, argue that these risks are greatly exaggerated. *See*, *e.g.*, Thomas Rid, *Cyber War Will Not Take Place*, 35 JOURNAL OF STRATEGIC STUDIES 5 (2012).

This article examines these questions through three lenses: (1) a legal perspective, to examine the range of reasonable interpretations of self-defense rights as applied to cyber attacks, and the relative merits of interpretations within that range; (2) a strategic perspective, to link a purported right of armed self-defense to long-term policy interests including security and stability; and (3) a political perspective, to consider the situational context in which government decisionmakers will face these issues and predictive judgments about the reactions to cyber crises of influential actors in the international system.

My main point is that these three perspectives are interrelated, so lawyers interested in answering these questions should incorporate the strategic and political dimensions in their analysis.[2] This is not just to make the banal, generic point that politics, strategy and law are interrelated. Of course they are. Rather, this article aims to show specifically how development of politics, strategy and law will likely play out interdependently with respect to this particular threat—cyber attacks—and to draw some conclusions about legal development in this area from that analysis.

The focus of this essay on military self-defense to cyber attacks (that is, self-defense in a legal sense of resort to force) is not meant to suggest that this is the most important element of a comprehensive cybersecurity strategy—far from it. Most attention these days is properly on other components of that strategy, including better network security and "offensive" cyber measures, though military force is part of the strategic tool set. Also, an important caveat is that this analysis is self-consciously colored with an American perspective. If one assumes, as I do, though, that legal analysis and development cannot be divorced from strategy and politics, then America's power—in its various forms—and vulnerabilities to power will greatly influence its own interpretive approach to these issues, and because of its relative power globally it will greatly influence international legal movement in this area.

II. LEGAL PERSPECTIVE

A legal perspective on the question of cyber attacks as armed attacks sees the issue as one of self-defense rights under the *jus ad bellum* framework. Article 2(4) of the UN Charter mandates that "[a]ll Members shall refrain

2. This essay draws heavily on a previous article: Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421 (2011).

in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[3] Article 51 then provides, however, that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations."[4] A legal question then arises: when, if ever, is a cyber attack an "armed attack" such that it triggers self-defense rights?

No consensus answer yet exists to this question, and several analytic approaches are competing for adherents.[5] A strict reading of "armed attack" would confine its meaning to kinetic violence, as opposed to non-physical violence or harm with no physical damage (take, for example, economic or diplomatic sanctions), and cyber attacks might therefore be considered as unable ever—on their own—to trigger armed self-defense rights. This position offers a bright-line rule that is relatively easily applied, but it is difficult to square with the treatment of chemical or biological weapons attacks (which everyone would acknowledge as an armed attack) and fails to account for new cyber vulnerabilities. The position is therefore rarely advanced that a cyber attack could *never* constitute an armed attack.

A more common starting point for analysis is to consider the effects or consequences of a cyber attack in determining whether it crosses the threshold of "armed attack." That is, the essence of an "armed attack" and the resulting self-defense right is the direct or perhaps indirect result of a hostile action—typically, but not necessarily, in the form of kinetic violence—and legal interpretation should proceed by examining whether the results of a specific cyber attack are sufficiently like kinetic violence.[6]

Among those taking an effects-based approach to Article 51 is a further

---

3. U.N. Charter art. 2, para. 4.

4. *Id.*, art. 51.

5. For a discussion of these positions, see Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIFORNIA LAW REVIEW 817, 841–49 (2012).

6. *See* NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 33–34 (William A. Owens et al. eds., 2009) [hereinafter NRC REPORT]; Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thought on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 914–15 (1999); Katharina Ziolkowksi, *Computer Network Operations and the Law of Armed Conflict*, 49 MILITARY LAW & THE LAW OF WAR REVIEW 47, 69–75 (2010); TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 92–95 (Michael N. Schmitt ed., 2013), draft *available at* http://issuu.com/nato_ccd_coe/docs/tallinn_manual_draft /1#share.

split in method. Some legal experts have suggested that to qualify as an armed attack a cyber attack must produce *violent* consequences of the sort usually produced by bombs or bullets.[7] So, for example, a cyber attack that caused a power station to explode or one that caused airplanes to crash could legally constitute an armed attack, but cyber attacks that cause economic or social damage—like taking down the stock market or bringing transportation systems to a halt—could not. Many other legal experts take a broader view of what sort of effects could constitute an armed attack, arguing that to focus on death or physical damage fails to account for modern society's critical reliance on information infrastructure and connectivity.[8] They would, therefore, look beyond just the type of effect to its magnitude, immediacy and other factors in assessing whether a cyber attack crosses the self-defense threshold.

Any effects-based interpretive approach leads to difficult secondary questions. These include how to calculate proportionality of an armed response (especially given that the effects of cyber attacks may be difficult to measure and direct causality may be difficult to assess); how to judge imminence for the purposes of anticipatory self-defense (given that discerning cyber attacks from other cyber activities, like espionage, is so difficult and that once launched some attack sequences take place in split seconds); and how to consider State responsibility (given that attacks may be launched by individuals or groups with loose relationships to States).

The United States government has generally followed an effects-based approach, though only gradually providing information publicly about the way in which it does or would legally assess cyber attacks' effects. In testifying before the Senate committee considering his nomination to head the new U.S. Cyber Command, Lieutenant General Keith Alexander explained that "[t]here is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what con-

---

7. *See*, *e.g.*, Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (Vol. 76, U.S. Naval War College International Law Studies).

8. *See* NRC REPORT, *supra* note 6, at 253–54 (arguing that the traditional legal emphasis on death or physical damage is problematic because "modern society depends on the existence and proper functioning of an extensive infrastructure that itself is increasingly controlled by information technology," and that therefore "[a]ctions that significantly interfere with the functionality of that infrastructure can reasonably be regarded as uses of force, whether or not they cause immediate physical damage").

stitutes a use of force."[9] He went on, however, to suggest that "[i]f the President determines a cyber event does meet the threshold of a use of force/armed attack, he may determine that the activity is of such scope, duration, or intensity that it warrants exercising our right to self-defense and/or the initiation of hostilities as an appropriate response."[10]

More recently, the White House stated in its official cybersecurity strategy that "[c]onsistent with the United Nations Charter, states have an inherent right to self-defense that may be triggered by certain aggressive acts in cyberspace."[11] It went on to declare:

> When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners. We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests.[12]

Without expressly endorsing an effects-based legal analysis or explaining the details of that analysis, the United States hereby appears to be relying on it in asserting the same self-defense authority universally recognized as applying to conventional armed attacks. As with any armed attack, the United States is declaring its view that some cyber attacks open the full range of self-defensive instruments; a cyber attack will not necessarily be met with responses confined to the cyber realm or other measures short of armed force.

Offering a bit more detail as to its legal position on this, in 2011 the United States explained its interpretation of Article 51 to the UN Group of Global Experts in the following terms:

---

9. Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command: Before the S. Armed Services Comm., 111th Cong. 11 (Apr. 15, 2010), http://www.armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf.

10. *Id.* at 12.

11. THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 10 (2011).

12. *Id.* at 14.

> It may be difficult to reach a definitive legal conclusion as to whether a disruptive activity in cyberspace constitutes an armed attack triggering the right to self-defence. For example, where the threat actor and the motive are unknown, and effects result that do not directly cause substantial death or physical destruction, it may be possible to reach differing conclusions about whether an armed attack has occurred. However, such ambiguities and room for disagreement do not suggest the need for a new legal framework specific to cyberspace. Instead, they simply reflect the challenges in applying the Charter framework that already exists in many contexts.[13]

Nevertheless, the U.S. statement concludes that "under some circumstances, a disruptive activity in cyberspace could constitute an armed attack."[14]

In September 2012, State Department Legal Advisor Harold Koh elaborated a little further the U.S. position in a public address, explaining that some cyber attacks could constitute a prohibited use of force:

> *Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.* In assessing whether an event constituted a use of force in or through cyberspace, we must evaluate factors including: the context of the event, the actor perpetrating the action (recognizing challenging issues of attribution in cyberspace), the target and location, effects and intent, among other possible issues. Commonly cited examples of cyber activity that would constitute a use of force include, for example: (1) operations that trigger a nuclear plant meltdown; (2) operations that open a dam above a populated area causing destruction; or (3) operations that disable air traffic control resulting in airplane crashes.[15]

He went on to explain the long-standing U.S. position that any such use of force could potentially trigger self-defense rights as an armed attack.[16]

At the time of this writing, some U.S. allies have moved cautiously in this general direction through public statements, while some other power-

---

13. *See* U.N. Secretary-General, Replies to the Developments in the Field of Information and Telecommunications in the Context of International Security: Report of the U.N. Secretary-General 18, U.N. Doc. A/66/152 (July 15, 2011).

14. *Id.*

15. Harold Hongju Koh, Remarks at the U.S. Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012), http://www.state.gov/s/l/releases/remarks/197924.htm (emphasis in original).

16. *Id.*

ful States have expressed concern about it. In 2012, for instance, the British Armed Forces Minister stated in response to parliamentary questioning that a cyber attack like that suffered by Estonia in 2007—which was widely blamed on Russia and which caused massive economic and social disruption—might trigger NATO's collective self-defense provisions.[17] NATO as a collective body has been working on a joint approach to cybersecurity, though NATO's official rhetoric in the field of self-defense has been quite cautious.[18] In 2011, the United States and Australia announced that their mutual defense treaty extends to cyberspace, signaling a joint intention to treat cyber attacks within the same cooperative framework as armed threats though without explicitly referencing an armed response.[19] Meanwhile, however, in diplomatic groupings China has resisted the idea that cyber attacks could trigger a traditional right of self-defense, urging instead new forms of international legal regulation and a broader understanding of cyber threats, to include Internet content threatening to regime stability, while Russia has advocated an international agreement to fill what it sees as gaps in international law with respect to cyber weapons.[20]

Despite calls from some circles that they urgently demand clear resolution, it is likely that legal questions about cyber attacks as armed attacks will be answered not through formal, multilateral instruments[21]—like a new treaty convention—but incrementally through State practice. That is, the law will evolve and adapt over time through the prevailing conduct and legal views expressed by States in planning for and responding to cyber-attack incidents.

---

17. *See UK Minister: Cyberattack Could Prompt NATO Action*, GUARDIAN (May 16, 2012), http://www.guardian.co.uk/world/feedarticle/10245167.

18. *See* NORTH ATLANTIC TREATY ORGANIZATION, STRATEGIC CONCEPT FOR THE DEFENCE AND SECURITY OF THE MEMBERS OF THE NORTH ATLANTIC TREATY ORGANIZATION ¶ 19 (2010), *available at* http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf (discussing the need to develop joint policies on cyber defense).

19. *See* Media Note, Office of the Spokesperson, U.S. Department of State, U.S.-Australia Ministerial Consultations 2011 Joint Statement on Cyberspace (Sept. 15, 2011), http://www.state.gov/r/pa/prs/ps/2011/09/172490.htm.

20. *See* Adam Segal & Matthew Waxman, *Why a Cybersecurity Treaty Is a Pipe Dream*, CNN (Oct. 26, 2011, 2:01 PM), http://globalpublicsquare.blogs.cnn.com/2011/10/27/why-a-cybersecurity-treaty-is-a-pipe-dream/.

21. *See* Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, *in* FUTURE CHALLENGES IN NATIONAL SECURITY AND LAW 5 (Peter Berkowitz ed., 2011), http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf; Segal & Waxman, *supra* note 20.

This means that legal evolution is likely to occur in significant part through defensive planning doctrine and declaratory policies issued in advance of actual cyber-attack crises, so to understand that development we need to rotate our analytic lens toward a strategic angle. In addition to the unilateral and joint self-defense policy statements cited earlier, for instance, Japan's national security agencies have reportedly been following the U.S. lead, generally accepting the U.S. legal interpretation of Article 51 with respect to cyber attacks in planning their defense.[22] Given Japan's reliance on U.S. security guarantees, this is not so surprising and illustrates the tight linkage between legal development and strategic relations.

Legal development is also likely to occur incrementally through actions and reactions of States and other major international actors during and following actual cyber-attack crises. This means we will need to rotate our analytic lens toward a political angle, too.

III. A STRATEGIC PERSPECTIVE

A strategic perspective on the question of cyber attacks as armed attacks sees the issue as one linking a purported right of armed self-defense to long-term policy interests—both national interests and global ones in the case of the United States—including security and stability. The substance and clarity of any such legal right has the potential to significantly enhance or detract from those strategic ends.

Armed self-defense to cyber attacks may be strategically valuable in several respects. First, anticipatory or responsive military actions might be important in some cases to protecting military and critical infrastructure vulnerable to cyber attacks—for example, by striking at facilities or individuals responsible for launching or directing them—though, because the physical infrastructure associated with cyber attacks may be quite small and widely dispersed, this sort of preventive use of force specifically to neutralize the possibility of initial or follow-on cyber attacks has not been the subject of much discussion. Second, the credible threat of self-defensive military actions might help deter cyber attacks by raising the prospective costs of hostile cyber activities in the minds of adversaries (though probably not much so of non-State adversaries, against whom deterrent threats of military action will not be very potent). Such strategic logic likely underlies the

22. *See Govt Claims Cyberdefense Right: Says International Laws Should Be Applied to Computer Infiltration*, DAILY YOMIURI ONLINE (May 17, 2012), http://www.yomiuri.co.jp/dy/national/T120516005387.htm.

U.S. declaratory postures described in the previous section, putting adversaries on notice that they should expect a possible military response to some cyber threats.

This is not the place to discuss in any detail the specific challenges and nuances of relying in part on military defense or deterrence against cyber attacks, a topic that many others have written about in detail.[23] The salient concern here is the way in which—to turn our lens back a bit and open the aperture to capture the legal and strategic perspectives together—legally regarding some cyber attacks to constitute armed attack might contribute strategically. It could do so in a number of ways.

For example, if one believes that armed self-defense is important to protecting against cyber attacks through anticipatory or responsive military actions, internally a well-established legal right helps strengthen the hand of political leaders weighing such options (an issue taken up further in the next session, which turns our lens toward a political perspective). An established or articulated right adds legitimacy to forceful options and may be taken as a guide of likely global reactions. A well-established right also facilitates military planning for such contingencies by clearing internal obstacles and bolstering the legitimacy and bureaucratic expectation of doing so. Within agencies charged with operationalizing them, it is much easier to plan and develop options for policy routes that are declared legal.

By thinking externally about the expectations of others, a legal right of armed self-defense might contribute to deterrence by establishing and communicating more emphatically and clearly red lines associated with self-defensive threats.[24] It helps to signal to others thresholds beyond which they should expect significant escalation, to include military means. When combined with rules of State responsibility, a right of armed self-defense might also induce States to crack down more strongly on cyber attacks launched from their territory, or perhaps to share more intelligence about cyber threats within their jurisdiction, whether out of a sense of legal obligation or for fear of being targeted with armed self-defense.

---

23. On the special difficulties of deterring cyber attacks, see MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 41–52 (2009); NRC REPORT, *supra* note 6, at 303; John Markoff, David E. Sanger & Thom Shanker, *In Digital Combat, U.S. Finds No Easy Deterrent*, NEW YORK TIMES, Jan. 26, 2010, at A1.

24. *See* James A. Lewis, *Multilateral Agreements to Constrain Cyberconflict*, ARMS CONTROL TODAY, June 2010, at 16; Adam Segal, *Cyberspace Governance: The Next Step*, Council on Foreign Relations Policy Innovation Memorandum No. 2 (Mar. 14, 2011), http://www.cfr.org/cybersecurity/cyberspace-governance-next-step/p24397.

These strategic benefits, however, must be balanced with strategic risks associated with legal treatment of some cyber attacks as armed attacks. Calibrating among such benefits and risks has always been a purpose and sustaining foundation of the *jus ad bellum* regime, and adapting it to this domain will be especially tricky.[25]

One strategic risk is the possibility of eroding normative constraints on war, shifting our focus back toward the legal perspective. As capabilities proliferate among State and non-State actors to conduct various sorts of malicious, hostile or intelligence-gathering activities in cyberspace, any deterrence value of treating them as armed attacks triggering self-defense rights under Article 51 might be outweighed by the dangers of lowering legal barriers to military force in a wider range of circumstances or conditions. Indeed, some would argue that the strategic value of promoting a right of armed self-defense against cyber attacks could turn out to be quite low—since, among other reasons that are discussed in the following section, it may be difficult to sufficiently prove one's case publicly in justifying military responses—while doing so may introduce greater insecurity and instability to the international system by eroding normative constraints on military responses to non-military harms.

Another strategic danger is that of miscalculated escalation: perhaps we want law to help stay the hand of political leaderships who might be inclined to overreact to cyber crisis with force. Rather than clearing the way—normatively and bureaucratically—for decisionmakers pressing for forceful responses, international law can play a role in promoting more thorough deliberation, even if one doubts that in extreme situations it imposes perfect constraints on powerful States. This again suggests the need to think about the strategy of cyber attacks as armed attacks while examining the issue through a political lens, too.

IV. A POLITICAL PERSPECTIVE

A political perspective considers the situational context in which political decision makers will face these issues and predictive judgments about the reactions to cyber-attack crises of influential actors in the international system. The politics of cyber attacks will undoubtedly be shaped by law and

25. *See* NRC REPORT, *supra* note 6, at 256 (discussing costs and benefits to preventing escalation in setting an appropriate threshold for self-defense).

strategy in this area, but no effective legal or strategic doctrine can be designed that does not account for the politics.

The domestic and international politics of a future cyber crisis are, of course, impossible to predict accurately. A few features of such cases are very likely to influence those politics, however. First, cyber-attack incidents will probably involve a publicly ambiguous set of facts. Conventional military attacks are usually quite visible—kinetic violence can be and often is broadcast widely, immediately and understandably—and the common experience of them makes political reactions fairly (though far from entirely) predictable. Malicious computer code or actions in cyberspace, by contrast, are opaque to public view, technically very complex and likely to emerge piecemeal.

Second, and closely related, responses and reactions to cyber attacks will probably involve high levels of government secrecy. The perpetrators of cyber attacks may try to keep their responsibility and methods secret. Defenders too, though, may be reluctant to disclose details or even the very existence of cyber attacks, whether to protect secrets about their vulnerabilities and defenses, prevent public panic, avoid political embarrassment, or escape unwanted domestic pressure to take retaliatory actions. Consider the case of Stuxnet and other cyber attacks against Iran's nuclear development program: press accounts report that the United States and Israel launched these attacks covertly—trying not only to mask their responsibility but to mask the very existence of a cyber attack—while Iran officially denied that it had been attacked or suffered any significant harm.[26]

Third, cyber-attack incidents will involve difficulties in proving attribution. It is hotly debated how effectively States can trace digital fingerprints of cyber attacks, which may be routed through many unwitting third parties' computer systems, back to their ultimate source, and it is widely believed that some States would conduct cyber attacks through loosely affiliated or unofficial private parties. As a purely technical matter, these attribution challenges may be overstated, especially for the United States and its premier intelligence and cyber-forensic capabilities. As a political matter, however, a critical issue is whether attacked States or their allies can demonstrate the aggressor's culpability to domestic and international audiences sufficiently to justify armed self-defense. There may be a significant

26. *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES, June 1, 2012, at A1.

gap between sufficiently establishing attribution for internal intelligence purposes and doing so for external justification of forceful responses.

A political upshot of these factors is that armed self-defense to a cyber attack will likely require quite a high minimum threshold of harm—probably a much higher quantum of harm than would be required if it were a conventional armed attack. Political decisionmakers will have a very difficult time rallying support at home and abroad for military responses to isolated cyber attacks that do not cause significant and publicly discernible damage, even though legal arguments might strengthen their hand in doing so. Whereas even low levels of hostile kinetic violence—say a barrage of small missiles that fail to detonate or cause much injury—will not only justify politically an armed response but may *demand* it politically, dud or stymied cyber attacks probably will not. Swiveling back to the legal perspective, this means that although legal line-drawing near the margins is very challenging for lawyers applying an effects-based analysis, it may not be quite so problematic in practice, because States are unlikely to respond to small-scale attacks with military force.

That said, it is also likely that very harmful cyber attacks for which armed self-defense is an option will occur against the background of or in combination with other hostile activities. In other words, and considering also the strategic perspective, there are likely to be few "naked" cases of cyber attacks—bolt-from-the-blue actions in the complete absence of other significant hostile actions or threats—against which political leaders will consider armed self-defense a viable response. States launching cyber attacks will likely be doing so in combination with other strategic acts, including militarily threatening moves. Non-State groups such as terrorist organizations against which military self-defense might make any sense will generally have already threatened other violence. Regardless of how such non-cyber moves and threats figure formally into a defending State's legal analysis, as a political matter they will no doubt figure significantly in its public justification of force.

V. CONCLUSIONS: LOOKING FORWARD

As the issue of cyber attacks as armed attacks is examined simultaneously through the three lenses—the legal, strategic and political—several general conclusions emerge. First, there is a range of reasonable interpretations of cyber "armed attacks" for the purposes of triggering militarily forceful self-defense, and a stable consensus is unlikely for the foreseeable

future. One reason for this legal instability is that strategic asymmetries pull interpretation in different directions.[27] I previously stated it this way:

> The United States appears to be placing its legal bets on a future world in which it can continue to rely partly on its comparative military edge to deter cyber-attacks while supplementing that deterrence with its own offensive, defensive, and preemptive cyber-capabilities—a bet that plays to some advantages but also carries risks. Reaching legal consensus with other major powers on these issues will be difficult in part because they perceive a different combination of strategic risks and opportunities. Therefore, U.S. policymakers should prepare to operate in a highly contested and uncertain international legal environment.[28]

The legal positions between States—and even within States—may shift over time as offensive advantages and defensive vulnerabilities shift. Moreover, international law regulating force changes very slowly, while the information technology creating these strategic opportunities and risks will continue to evolve rapidly.

Second, incremental legal development through State practice will be especially difficult to assess because of several features of cyber attacks. Actions and counteractions with respect to cyber attacks will lack the transparency of most other forms of conflict, sometimes for technical reasons but sometimes for political and strategic reasons. It will be difficult to develop consensus understandings even of the fact patterns on which States' legal claims and counterclaims are based, assuming those claims are leveled publicly at all, when so many of the key facts will be contested, secret, or difficult to observe or measure. Furthermore, the likely infrequency of "naked" cases of cyber attacks—outside the context of other threats or ongoing hostilities—means that there will be few opportunities to develop and assess State practice and reactions to them in ways that establish widely applicable precedent.

Finally, law can and should be used to support strategy in calibrating appropriate triggers and thresholds for self-defense, though the political features of cyber-attack crises—many of them directly linked to the technical features of cyber attacks—make doing so in advance more difficult than it has been with respect to conventional military threats. This means

---

27. On some of these asymmetries, see Thomas Rid, *Think Again: Cyberwar*, FOREIGN POLICY, Mar.–Apr. 2012, at 58.

28. Waxman, *supra* note 2, at 448–49.

that the adaptation of international law and the development among allies and partners of strategy to combat cyber threats go hand in hand. Those taking a more formalistic method to self-defense law may view this approach to legal interpretation as too malleable and subordinating of law to power politics. But any legal approach that fails to account for the strategic and political dynamics of cyber attacks is unlikely to survive early encounters with those realities.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Territorial Sovereignty and Neutrality in Cyberspace

Wolff Heintschel von Heinegg

89 INT'L L. STUD. 123 (2013)

Volume 89 2013

Territorial Sovereignty and Neutrality in Cyberspace

Wolff Heintschel von Heinegg[*]

I. INTRODUCTION

Because of its mystifying characteristics, cyberspace has been called a "fifth dimension" or a "fifth domain." There seems to be a widespread belief that it eludes the traditional rules and principles of international law, and that there is an urgent need for new rules specifically designed for cyberspace. All too often in the past we witnessed a considerable degree of perplexity vis-à-vis new technologies that resulted in similar desperate calls for new norms; however, only in rare cases were such calls justified. If analyzed soberly, international law as it currently exists need not capitulate to the novelty of the technology on which cyberspace is based or to the threats that did not exist prior to the cyber age. Interestingly, States seem to agree that customary international law is, in principle, applicable to cyber-

* Stockton Professor, U.S. Naval War College; Professor of Public Law, Europa-Universität Viadrina, Frankfurt (Oder), Germany. This article is a modified version of *Legal Implications of Territorial Sovereignty in Cyberspace* and *Neutrality in Cyberspace*, both articles published in 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT PROCEEDINGS 2012, at 1, 27 (Christian Czosseck, Rain Ottis & Kathartina Ziolkowski eds., 2012). The views expressed in this article are the sole responsibility of the author and do not reflect the view of the author's affiliations.

space, although there may be a need for a consensual adaptation to the specific characteristics of cyberspace.

This article will explore whether—and to what extent—the principle of territorial sovereignty and the law of neutrality apply to cyberspace. It will be shown that certain components of—and certain activities in—cyberspace are governed by the principle of territorial sovereignty and that neither general international law nor the law of neutrality has become obsolete merely because cyberspace may be considered a fifth dimension or part of the global commons.

II. TERRITORIAL SOVEREIGNTY

A. General Characteristics of Territorial Sovereignty

Under the principle of territorial sovereignty a State exercises full and exclusive authority over its territory.[1] As stated by Judge Max Huber in the *Palmas Island* arbitration award, "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusivity of any other States, the functions of a State."[2] The International Court of Justice (ICJ) has emphasized that "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations."[3] Territorial sovereignty, therefore, implies that, subject to applicable customary or conventional rules of international law, the State alone is entitled to exercise jurisdiction, especially by subjecting objects and persons within its territory to domestic legislation and to enforce these rules. Moreover, the State is entitled to control access to and egress from its territory. The latter right seems to also apply to all forms of communication. Finally, territorial sovereignty protects a State against any form of interference by other States. While such interference may amount to a use of force, this article does not address that issue.

It must be remembered that territorial sovereignty is relative in character insofar as it does not merely afford protection to States, but also imposes obligations on States, especially the "obligation to protect within the ter-

1. *See, e.g.*, S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18–20 (Sept. 7) [hereinafter *Lotus*]; Free Zones of Upper Savoy and Gex (Fr. v. Switz.), 1932 P.C.I.J. (ser. A/B) No. 46, at 166–68 (June 7).

2. Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

3. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 6, 35 (Apr. 9) [hereinafter *Corfu Channel*].

ritory the rights of other States, in particular their right to integrity and inviolability in peace and in war, together with the rights which each State may claim for its nationals in foreign territory."[4]

B. Territorial Sovereignty and Cyberspace

"Cyberspace" has been defined as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[5] There is a widely held view that it "is not a physical place—it defies measurement in any physical dimension or time space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the World Wide Web."[6] It is true that cyberspace is characterized by anonymity and ubiquity.[7] It seems logical, therefore, to assimilate it to the high seas, international airspace or outer space,[8] that is, to consider it a "global common" or, legally, a *res communis omnium*.[9] However, these characterizations merely lead to the obvious

4. Island of Palmas, *supra* note 2, at 839. In his separate opinion in the *Corfu Channel* case, Judge Alvarez stated, "By sovereignty, we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States. Sovereignty confers rights upon States and imposes obligations upon them." *Corfu Channel*, *supra* note 3, at 43.

5. Joint Chiefs of Staff, Joint Publication 1-02, DOD Dictionary of Military and Associated Terms (Nov. 8, 2010), as amended through July 15, 2012, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf [hereinafter Dictionary of Military and Associated Terms]. See also the definition by Arie J. Schaap, *Cyber Warfare Operations: Development and Use under International Law*, 64 AIR FORCE LAW REVIEW 121, 126 (2009) (a "domain characterized by the use of [computers and other electronic devices] to store, modify, and exchange data via networked systems and associated physical infrastructures").

6. THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 17 (2000).

7. It has been rightly stated that "global digital networks have the features they do—of placelessness, anonymity, and ubiquity—because of politics, not in spite of them." *See* Geoffrey L. Herrera, Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space 12 (2006) (paper prepared for the 47th Annual International Studies Association Convention March 22–25, 2006), http://www.allacademic.com/meta/p98069_index.html.

8. For an analysis to that effect, see Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 AIR FORCE LAW REVIEW 1, 17–42 (2009).

9. U.S. Department of Defense, Department of Defense Strategy for Operating in Cyberspace (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf [here-

conclusion that cyberspace in its entirety is not subject to the sovereignty of a single State or group of States—that it is immune from appropriation.

Despite the correct classification of "cyberspace as such" as a *res communis omnium*, State practice provides sufficient evidence that components of cyberspace are not immune from territorial sovereignty nor from the exercise of State jurisdiction. States have exercised, and will continue to exercise, their criminal jurisdiction over cyber crimes[10] and they continue to regulate activities in cyberspace. Moreover, the simple truth that "cyberspace requires a physical architecture to exist"[11] may not be disregarded. The equipment constituting the architecture is usually located within the territory of a State. It is owned by the government or by corporations; it is connected to the national electric grid.[12] The integration of physical components of cyber infrastructure located within a State's territory into the "global domain" of cyberspace cannot be interpreted as a waiver of the exercise of territorial sovereignty. While, in view of the genuine architecture of cyberspace, it may be difficult to exercise sovereignty, the technological and technical problems involved do not prevent a State from exercising its jurisdiction over the cyber infrastructure located in areas in its sovereign territory. States have, in fact, continuously emphasized their right to exercise control over such infrastructure, to assert their jurisdiction over cyber activities on their territory and to protect their cyber infrastructure against transborder interference by other States or by individuals.[13]

---

inafter DoD Strategy for Operating in Cyberspace] ("DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential."). *See also* U.S. Department of Defense, The Strategy for Homeland Defense and Civil Support 12 (2005), *available at* http://www.defense.gov/news/Jun2005/d20050630homeland.pdf ("The global commons consist of international waters and airspace, space, and cyberspace.").

10. *See, e.g.,* Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185.

11. Franzese, *supra* note 8, at 33.

12. *See* Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 AIR FORCE LAW REVIEW 43, 64 (2009).

13. *See* DoD Strategy for Operating in Cyberspace, *supra* note 9. *See also* U.S. Department of Defense, Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, at 7–8 (2011), *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf [hereinafter Cyberspace Policy Report]; THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 12–15 (2011), *available at* http://www.

It needs to be emphasized that the applicability of the principle of sovereignty to the components of, and activities in, cyberspace is not barred by the innovative and novel character of the underlying technology. This holds true for the majority of rules and principles of customary international law. In the 2011 International Strategy for Cyberspace, the Obama administration rightly stated that the "development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace."[14]

This does not necessarily mean that the rules and principles of international law are applicable to cyberspace in their traditional interpretation. Because of the novel character of cyberspace, and in view of the vulnerability of cyber infrastructure, there is a noticeable uncertainty among governments and legal scholars as to whether the traditional rules and principles are sufficient to provide answers to some worrisome questions. It is, therefore, of utmost importance that States agree not only on the application of customary international law to cyberspace, but also on a common interpretation of that law that takes into due consideration the "unique attributes of networked technology."[15] As called for in the International Strategy for Cyberspace, it is necessary that governments "continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace."[16]

---

whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter INTERNATIONAL STRATEGY FOR CYBERSPACE].

14. INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 13, at 9.

15. "Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them." *Id.*

16. *Id. See also* Cyberspace Policy Report, *supra* note 13, at 7 ("The United States is actively engaged in the continuing development of norms of responsible state behavior in cyberspace, making clear that as a matter of U.S. policy, long-standing international norms guiding state behavior also apply equally in cyberspace. Among these, applying the tenets of the law of armed conflict are critical to this vision, although cyberspace's unique aspects may require clarifications in certain areas."). The report emphasizes that the "law of armed conflict and customary international law . . . provide a strong basis to apply such norms to cyberspace governing responsible state behavior." *Id.* at 9.

C. Scope of Territorial Sovereignty in Cyberspace

The general applicability of the principle of territorial sovereignty to cyberspace encompasses that cyber infrastructure located on a State's land area, in its internal waters, territorial sea and, where applicable, archipelagic waters, and in national airspace.[17] Thus, in principle, the State is entitled to exercise control over cyber infrastructure and cyber activities in those areas. It must be kept in mind, however, that the exercise of sovereignty may be restricted by customary or conventional rules of international law, such as the immunity of diplomatic correspondence[18] and the rights of innocent passage, transit passage and archipelagic sea lanes passage.[19]

1. Geographic Scope (*Ratione Loci*)

After this identification of the areas in which the principle of territorial sovereignty applies, the first consequence is that cyber infrastructure located in those areas is protected against interference by other States. This protection is not limited to interference amounting to an unjustified use of force, to an armed attack or to a prohibited intervention.[20] Rather, because the interference constitutes an exercise of that State's jurisdiction, any activity attributable to it is considered a violation of the sovereignty of the territorial State.[21] This, *a fortiori*, holds true if the conduct has negative impacts on the integrity or function of another State's cyber infrastructure. However, not all State conduct that impacts on the cyber infrastructure of another State necessarily constitutes a violation of the principle of territorial sovereignty. If the act of interference results in inflicting material damage

17. Note that within the exclusive economic zone and on the continental shelf coastal States do not enjoy territorial sovereignty, but merely certain "sovereign rights" with respect to the natural resources in those sea areas. U.N. Convention on the Law of the Sea arts. 56, 77, Dec. 10, 1982, 1833 U.N.T.S. 3 [hereinafter LOS Convention].

18. Vienna Convention on Diplomatic Relations art. 27(1), Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95. Computers and computer networks located in the diplomatic mission are protected by Article 22.

19. LOS Convention, *supra* note 17, arts. 17–26, 37–42, 45, 52–53.

20. It is important to note that the prohibitions on the use of force and intervention only apply to States, i.e., to conduct attributable to a State. However, Article 51 of the UN Charter does not refer to the source of an armed attack giving rise to the "inherent right of self-defense." Today there is general agreement that the right applies to armed attacks by both State and non-State actors.

21. *See, e.g.*, 1 OPPENHEIM'S INTERNATIONAL LAW ¶ 123 (Robert Jennings & Arthur Watts eds., 9th ed. 1992).

to the cyber infrastructure, there seems to be a general consensus that such an act constitutes a violation of the sovereignty of the target State.[22] According to some, the damage inflicted must be not just material but severe.[23] If, however, there is no material damage or merely minor damage, it is unsettled whether that activity can be considered a violation of territorial sovereignty.[24] Those who hold that material damage is required usually cite espionage, including cyber espionage, as an example of an activity that is not a violation, because international law does not prohibit espionage. The fact that the data resident in the target system are modified by the act of intrusion is not considered sufficient to characterize cyber espionage as a prohibited violation of territorial sovereignty. It could be argued, however, that damage is irrelevant and the mere fact that a State has intruded into the cyber infrastructure of another State should be considered an exercise of jurisdiction on foreign territory, which always constitutes a violation of the principle of territorial sovereignty.

The International Strategy for Cyberspace indicates the following activities may qualify as violations of territorial sovereignty: attacks on networks; exploitation of networks; and other hostile acts in cyberspace that threaten peace and stability, civil liberties and privacy.[25] While the specific natures of those activities are not indicated, it seems that the U.S. government is advocating a rather wide scope of the principle of territorial sovereignty in asserting the right to counter such acts with all necessary means, including, if necessary, the use of conventional force.

It is irrelevant whether the cyber infrastructure protected by the principle of territorial sovereignty belongs to or is operated by governmental institutions, private entities or private individuals. Moreover, such infrastructure is also protected if it is located on board aircraft, vessels or other platforms enjoying sovereign immunity.[26] The provisions of the Outer Space

---

22 *Id.*, ¶ 119.

23. This is in recognition of the fact that the use by a State of its territory very often causes negative effects on the territory of neighboring States. Since the principle of territorial integrity is not considered to be absolute in character there are good reasons to maintain that damage below the threshold of severity must be tolerated and when such damage occurs it does not violate the territorial sovereignty or integrity of the affected State.

24. Those who consider damage as relevant will not classify those activities as violations of territorial sovereignty.

25. INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 13, at 12–14.

26. *See, e.g.*, LOS Convention, *supra* note 17, art. 95 ("warships on the high seas have complete immunity from the jurisdiction of any State other than the flag State"). Under Article 96 of the Convention "ships owned or operated by a State and used only for gov-

Treaty[27] and the Liability Convention[28] appear to support the conclusion that space objects operated exclusively for non-commercial government purposes also enjoy sovereign immunity.[29] While there is no treaty rule explicitly according sovereign immunity to all objects used for non-commercial government purposes, Article 5 of the UN Convention on State Immunity[30] importantly provides that a State enjoys immunity from the jurisdiction of the courts of another State with regard to its property.[31] This provision, along with the other treaties and rules just cited, provides sufficient evidence of a general principle of public international law according to which objects owned by a State or used by that State for exclusively non-commercial government purposes are an integral part of the State's sovereignty and are subject to the exclusive jurisdiction of that State if located outside the territory of another State.

"Sovereign immunity" means that any interference with an object enjoying such immunity constitutes a violation of the sovereignty of that State.[32] It must be borne in mind, however, that in times of international armed conflict the principle of sovereign immunity plays no role in relations between the belligerent States. During such conflicts objects enjoying

---

ernment non-commercial service" have the same immunity. With regard to State aircraft in international airspace, there is general consensus that they also enjoy sovereign immunity. *See* PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, COMMENTARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE rule 1(cc), cmt. to rule 1(cc), ¶ 6 (2010), *available at* http://ihlresearch.org/amw/Commentary%20on%20the%20HPCR%20Manual.pdf%20[hereinafter HPCR MANUAL].

27. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 610 U.N.T.S. 205.

28. Convention on International Liability for Damage Caused by Space Objects, Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187.

29. Space objects, such as satellites used for governmental and commercial purposes either by the State of registry or by that State in cooperation with a private corporation, do not enjoy sovereign immunity.

30. U.N. Convention on Jurisdictional Immunities of States and Their Property**,** G.A. Res. 59/38, annex, U.N. GAOR, 59th Sess., Supp. No. 49, U.N. Doc. A/59/49 (Dec. 16, 2004).

31. For an assessment, see David P. Stewart, *Current Developments: The UN Convention on Jurisdictional Immunities of States and Their Property*, 99 AMERICAN JOURNAL OF INTERNATIONAL LAW 194, 195–207. (2005).

32. For a first finding with regard to the sovereign immunity of warships, see the award of the Anglo-American Claims Commission in the *Jessie* case. Owners of the *Jessie*, the *Thomas F. Bayard* and the P*escawha* (Gr. Brit. v. U.S.), 6 R.I.A.A. 57 (1921), Reports: Neilsen's 479 (1926).

sovereign immunity may be destroyed if they qualify as lawful targets or are subject to seizure as booty of war[33] by the enemy's armed forces. Moreover, sovereign immunity is not limitless. For instance, the U.S. drone captured by Iran in December 2011 (allegedly downed by cyber means) had probably been in Iran's national airspace, thus violating Iran's territorial sovereignty.[34] Hence, Iran was entitled to use all necessary means, including cyber means, to terminate that violation.

Vessels and aircraft that do not exclusively serve non-commercial governmental purposes do not enjoy sovereign immunity. This doesn't mean, however, they are not protected when located in areas or spaces not covered by the territorial sovereignty of any State. While they cannot be considered an integral component of a State's sovereignty, they are included within the protective scope of that sovereignty by the link of nationality. Hence, the State of nationality exercises exclusive jurisdiction over such vessels and aircraft when they are located on the high seas or in international airspace. Accordingly, any interference with them constitutes a violation of the sovereignty of the State of nationality unless justified by a rule of international law. This also applies to space objects. It is prohibited under the Outer Space Treaty[35] to interfere with the activities of other States in the peaceful exploration and use of outer space. It is immaterial whether the space object is owned or operated by the government or by a private corporation. On the high seas and in international airspace the cyber infrastructure will regularly be located on board a vessel or aircraft. The determination of the State whose sovereignty and jurisdiction apply will depend on either following the flag-State principle[36] or on the registration of the aircraft.[37] Nationality of space objects is also determined by registration.[38]

---

33. *See* Yoram Dinstein, *Booty in Warfare*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (Rüdiger Wolfrum ed., 2012), http://www.mpepil.com/subscriber_article?script=yes&id=/epil/entries/law-9780199231690-e256&recno=4&author=Dinstein%20%20Yoram [hereinafter MAX PLANCK ENCYCLOPEDIA].

34. For competing views of the circumstances of the capture, see, e.g., David Axe, *Nah, Iran Probably Didn't Hack CIA's Stealth Drone*, WIRED (Apr. 24, 2012, 12:00 PM), http://www.wired.com/dangerroom/2012/04/iran-drone-hack/; Mathew J. Schwartz, *Iran Hacked GPS Signals to Capture U.S. Drone*, INFORMATION WEEK (Dec. 16, 2011, 12:30 PM), http://www.informationweek.com/security/attacks/iran-hacked-gps-signals-to-capture-us-dr/232300666.

35. *Supra* note 27.

36 LOS Convention, *supra* note 19, art. 92.

37. *See* Convention on International Civil Aviation art. 17, Dec. 7, 1944, 15 U.N.T.S. 295 ("[a]ircraft have the nationality of the State in which they are registered").

2. Exercise of Jurisdiction (*Scope Ratione Materiae*)

The second consequence of the applicability of the principle of territorial sovereignty to the components of cyberspace is the wide-ranging right of the territorial State (including the flag State and the State of registry) to exercise its jurisdiction over cyber infrastructure and over cyber activities.

The concept of jurisdiction may be understood in a broad sense as referring to a State's "lawful power to act and hence to its power to decide whether and, if so, how to act, whether by legislative, executive or judicial means. In this sense, jurisdiction denominates primarily, but not exclusively, the lawful power to make and enforce rules."[39] As has already been noted, the exercise of jurisdiction is not limited to a State's territory. For instance, a State exercises exclusive jurisdiction on board vessels flying its flag and on board aircraft registered in that State. Moreover, according to the principles of active and passive nationality, a State is entitled to exercise its jurisdiction over the conduct of individuals that occurred outside its territory. Under the universality principle, the same holds true even if neither the perpetrator nor the victim is a national of the State in question. Finally, the exercise of jurisdiction can be based upon the protective principle.[40]

For the purposes of this article, the jurisdictional bases just listed, although of importance in the cyber domain, need not be addressed; the focus will be on the scope of territorial jurisdiction.

It may be noted in this context that territorial jurisdiction does not necessarily presuppose territorial sovereignty. For instance, a State may exercise exclusive jurisdiction over territory leased or occupied.[41] Jurisdiction conferred on coastal States in their exclusive economic zones or on their continental shelves, although it may be conceived of as quasi-territorial in character, is only analogous to territorial jurisdiction *strictu sensu*, because it is limited to certain prescribed activities.

The State's right to exercise its jurisdiction, that is, to proscribe, enforce and adjudicate activities of objects and persons physically or legally present in its territory, seems to be undisputed unless otherwise limited by applica-

38. *See* Convention on Registration of Objects Launched into Outer Space, Jan. 14, 1973, 28 U.S.T. 695, 1023 U.N.T.S. 15.

39. Bernard H. Oxman, *Jurisdiction of States* ¶ 1, *in* MAX PLANCK ENCYCLOPEDIA, *supra* note 23, http://www.mpepil.com/subscriber_article?script=yes&id=/epil/entries/law-9780199231690-e1436&recno=1&author=Oxman Bernard H.

40. For a discussion of the different bases of jurisdiction, see *id.*, ¶¶ 11–45.

41. *Id.*, ¶ 15.

ble rules of international law, probably including human rights law. Cyber infrastructure located within the territory of a State, and cyber activities occurring therein, are susceptible to almost unlimited proscriptive and enforcement measures by the State. Territorial jurisdiction includes the right of a State to regulate, restrict or prohibit access to its cyber infrastructure, whether access is gained from within or without its territory. It must be reemphasized that integration of the physical components of cyber infrastructure located within a State's territory into the "global domain" of cyberspace does not constitute a waiver of the exercise of territorial sovereignty and jurisdiction. In view of the mobility of users and of cloud- or grid-distributed systems, it may often be very difficult to effectively exercise territorial jurisdiction. Still, those difficulties do not justify the conclusion that territorial jurisdiction, if applied to cyberspace, is but a "toothless tiger." To the contrary, States have regularly and quite successfully—while not always applauded—proven their willingness and determination to enforce their domestic law over a variety of cyber activities.

A specific feature of territorial jurisdiction is the so-called effects doctrine, under which a State is entitled to exercise its jurisdiction over a conduct occurring outside its territory that produces effects in its territory.[42] A useful explanation of that doctrine has been provided in a European Court of Justice judgment:

> The two undisputed bases on which State jurisdiction is founded under international law are territoriality and nationality. The former confers jurisdiction on the State in which the person or the goods in question are situated or the event in question took place. The latter confers jurisdiction over nationals of the State concerned.
>
> Territoriality itself has given rise to two distinct principles of jurisdiction:
>
> (i) subjective territoriality, which permits a State to deal with acts which originated within its territory, even though they were completed abroad;
>
> (ii) objective territoriality, which, conversely, permits a State to deal with acts which originated abroad but which were completed, at least in part, within its own territory. . . .

42. *Id.*, ¶¶ 22–26.

> [The effects doctrine] confers jurisdiction upon a State even if the conduct which produced [the effects] did not take place within its territory.[43]

Applied to the cyber domain, the effects doctrine may give rise to the exercise of jurisdiction over individuals who have conducted cyber operations against the cyber infrastructure in another State.[44]

In summary, the principle of territorial sovereignty, and the ensuing right of a State to exercise its territorial jurisdiction, applies to cyberspace insofar as the cyber infrastructure is located within its territory or on platforms over which the State exercises exclusive jurisdiction. Territorial sovereignty and territorial jurisdiction also apply to individuals present in the State and to conduct that either takes place within that territory or produces harmful effects therein. The exercise of jurisdiction under any of the recognized bases of international law is limited only if there exist explicit rules to that effect. Thus, the characteristics of cyberspace do not pose an obstacle to the exercise of territorial sovereignty and jurisdiction; they merely increase the difficulty of so doing.

D. Obligations of States in Cyberspace and the Issue of Attributability

1. Obligations of States in Cyberspace[45]

As noted previously, the principle of territorial sovereignty not only protects States by affording them exclusive rights, but also imposes obligations on them.[46] The protective scope of those obligations serves to protect the territorial sovereignty and integrity of other States.

---

43. Joined Cases C-89, 104, 114, 116–117, 125–129/85, A. Ahlström Osakeyhtio v. Comm'n, 1988 E.C.R. 5193, ¶¶ 19–21 (citation omitted), *available at* http://eur-lex.europa.eu/staging/LexUriServ/LexUriServ.do?uri=CELEX:61985CC0089:EN:HTML.

44. Hence, irrespective of the issue of attribution, Estonia would be entitled to exercise its criminal and civil jurisdiction over those individuals who conducted the distributed denial-of-service attacks against the Estonian cyber infrastructure in 2007.

45. This section does not deal with the entire spectrum of obligations States are to observe in cyberspace; therefore, the prohibition of the use of force and the issue of "armed attack" are not addressed.

46. See the references *supra* note 4 and accompanying text.

a. Duty of Prevention

The principle of territorial sovereignty entails an obligation imposed on all States to respect the territorial sovereignty of other States. As the ICJ held in its *Nicaragua* decision, "'Between independent States, respect for territorial sovereignty is an essential foundation of international relations,' and international law requires political integrity also to be respected."[47]

The obligation to respect the territorial sovereignty of other States applies to conduct that is attributable to a State. Additionally, in the *Corfu Channel* judgment, the ICJ held that respect for the territorial sovereignty of other States implies the obligation of every State "not to allow knowingly its territory to be used for acts contrary to the rights of other States."[48] Accordingly, a State is required under international law to take appropriate actions to protect the interests of other States.[49] This obligation is not limited to prevention of "criminal acts,"[50] but applies to all activities inflicting severe damage—or that have the potential to inflict such damage—on persons and objects protected by the territorial sovereignty of the target State.[51]

In the context of cyber attacks, the duty of prevention has been correctly summarized as follows: "States have an affirmative duty to prevent cyberattacks from their territory against other states. This duty actually encompasses several smaller duties, to include . . . prosecuting attackers, and, during the investigation and prosecution, cooperating with the victim-states

47. Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S), 1986 I.C.J. 14, ¶ 202 (June 27), citing its judgment in the *Corfu Channel* case. *Corfu Channel*, *supra* note 3, at 35.

48. *Corfu Channel*, *supra* note 3, at 22.

49. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, ¶ 68 (May 24). *See also* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 215–16 (5th ed. 2011).

50. Michael N. Schmitt, *Preemptive Strategies in International Law*, 24 MICHIGAN JOURNAL OF INTERNATIONAL LAW 513, 540–41 (2003).

51. In the famous *Trail Smelter* case, the Tribunal held, *inter alia*:

> "This right (sovereignty) excludes . . . not only the usurpation and exercise of sovereign rights . . . but also an actual encroachment which might prejudice the natural use of the territory and the free movement of its inhabitants. . . ." [U]nder the principles of international law . . . no State has the right to use or permit the use of its territory in such a manner as to cause injury . . . in or to the territory of another or the properties or persons therein, when the case is of serious consequence . . . .

Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1963, 1965 (Trail Smelter Arb. Trib. 1938 & 1941).

of cyberattacks that originated from within their borders."[52] The term "cyber attack" is often understood as comprising "remote intrusions into computer systems by individuals";[53] however, mere intrusions are not included, because they do not inflict direct material harm. Rather, mere intrusions must be considered acts of espionage.[54] Since all States engage in espionage, including via cyberspace, mere intrusions into foreign computers or networks are not covered by the prohibition on cyber attacks.

The duty of prevention presupposes knowledge. This does not necessarily mean actual knowledge; it also applies to cases of presumptive knowledge. A State will have actual knowledge if its organs have detected a cyber attack originating from its territory or if it has been informed by the victim-State that a cyber attack has originated from its territory. Knowledge is to be presumed if the cyber attack can reasonably be considered to belong to a series of cyber attacks. It is important to note the ICJ has held that even if "an act contrary to international law has occurred [on a State's territory], . . . it cannot be concluded from the mere fact of the control exercised . . . over its territory . . . that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein."[55]

Although it may be concluded that the duty of prevention does not apply if the State from whose territory the acts have been initiated has neither actual nor presumptive knowledge, this conclusion is not accepted by everyone. According to some authorities, the duty of prevention should be based on a State's "actions to prevent cyberattacks in general."[56] According to this position,

> States that do not enact [stringent criminal laws and undertake vigorous law enforcement] fail to live up to their duty to prevent cyberattacks. . . . A state's passiveness and indifference toward cyberattacks make it a sanctuary state from where attackers can safely operate. When viewed in this light, a state can be held indirectly responsible for cyberattacks . . . .[57]

---

52. Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent*, 201 MILITARY LAW REVIEW 1, 62 (2009).

53. *Id.* at 14.

54. *See, e.g.*, Schaap, *supra* note 5, at 139–40. *See also supra* notes 20–24 and accompanying text.

55. *Corfu Channel*, *supra* note 3, at 18.

56. Sklerov, *supra* note 52, at 71.

57. *Id.*

However, in this author's opinion, the theoretical possibility that a State that has not enacted criminal laws—when it has not been obliged to do so under an international treaty—may become a sanctuary for cyber attackers is certainly not sufficient to justify the inapplicability of the duty of prevention's requirement for actual or presumptive knowledge.

There are, though, circumstances that may be considered as sufficient to support the assumption that a State had—or ought to have had—knowledge of the conduct. Such circumstances may exist if a cyber attack has been launched from cyber infrastructure that is under exclusive government control and that is used only for non-commercial government purposes. Provided that the origin of the cyber attack can be traced back to the government's cyber infrastructure, there may be at least a rebuttable presumption that the State should have known of that use of its territory. It is important to note that a rebuttable presumption of knowledge does not mean that the conduct is attributable to the State. If it were, it would mean that the aggrieved State would be entitled to resort to countermeasures, including, when applicable, the use of force in response to an armed attack. The rebuttable presumption is not sufficient, however, either to attribute the conduct to the State or to serve as a legal basis for countermeasures, although that might be the case if the events were occurring in the physical world. Because of the difficulty of identifying the originator of a cyber attack, attributing it to the State whose cyber infrastructure was utilized could lead to escalation since the infrastructure may have been usurped by another State or by non-State actors, such as terrorists or other criminals. Additionally, allowing countermeasures on the basis of a "knows-or-should-have-known standard" would impose far-reaching prevention obligations on States that, given the nature of the technology involved, would be difficult, if not impossible, to fulfill.

In that regard, some might be inclined to recognize the duty of prevention as applying not just to cyber attacks launched from the territory of a State, but also to cyber attacks/cyber operations that are routed through the cyber infrastructure of another State. It is unsettled, however, whether the transit of data brings into operation the obligation of prevention even if the transit State knows, or should have known, of the use of its cyber infrastructure. While extending the prevention obligation to transit of data seems simple, those so advocating fail to recognize the complexity of cyberspace. For example, the transiting data may be harmless in and of themselves, but they may be part of a larger packet. While the larger packet, the constituent parts of which may be transmitted over different nodes, may be

considered a "cyber weapon," the transit State does not know this. Additionally, in most cases it would be meaningless to oblige the transit State to take preventive action, because the data may be rerouted, thus nevertheless arriving at their destination in the target State.

b. Further Obligations

Finally, State practice seems to justify the conclusion that there is a growing readiness of States to accept obligations that are of a more general character than the obligation to refrain from harmful conduct or to prevent such conduct.

For instance, the United States has taken the position that identifying the rules and principles of international law applicable to cyberspace must be guided by applying the "broad expectations of peaceful and just interstate conduct to cyberspace."[58] The U.S. cyberspace strategy emphasizes that States "need to recognize the international implications of their technical decisions, and act with respect for one another's networks and the broader Internet"[59] and demands that the emerging norms of cyberspace behavior be guided by five criteria, including global interoperability, network stability and cybersecurity due diligence.[60] Indeed, global interoperability, which is one of the main characteristics of the Internet, can only be preserved if "States . . . act within their authorities to help ensure the end-to-end interoperability of an Internet accessible to all."[61] Network stability presupposes that States do not "arbitrarily interfere with internationally interconnected infrastructure."[62] Since cybersecurity due diligence is understood to imply that "States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse,"[63] it may be considered as reflecting the obligation of prevention as it currently exists under customary international law. It is this author's belief that each of the criteria enumerated in the International Strategy for Cyberspace may not yet have attained that status, but they may well be accepted by a considerable number of States—at least by those that

58. INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 13, at 9.

59. *Id.* at 10.

60. *Id.* The remaining two criteria are "reliable access" and "multi-stakeholder governance."

61. *Id.*

62. *Id.*

63. *Id.*

are "like-minded." The criteria may, in any event, be considered to be of potentially norm-creating character, thus contributing to the progressive development of customary international law.

2. Attributability

Effective protection of territorial sovereignty in the cyber domain presupposes that particular conduct can be attributed to another State. The rather strict attributability criteria in Articles 4 to 11 of the International Law Commission's Draft Articles on State Responsibility[64] are designed for the purpose of determining State responsibility and do not necessarily preclude the application of more liberal criteria with a view to determining the origin of a cyber attack. It is, however, unclear whether States are prepared to agree on such criteria.

It is generally agreed that, in view of the architecture and characteristics of cyberspace, it is "virtually impossible to attribute a cyberattack during an attack. Although states can trace the cyberattack back to a computer server in another state, conclusively ascertaining the identity of the attacker requires an intensive, time-consuming investigation with assistance from the state of origin."[65] The cyber attacks on Estonia (2007) and on Georgia (2008) prove the correctness of this finding. The U.S. Department of Defense (DoD) has also stressed that because the "often low cost of developing malicious code and the high number and variety of actors in cyberspace make the discovery and tracking of malicious cyber tools difficult" and because "[m]ost of the technology used in this context is inherently dual-use, and even software might be minimally repurposed for malicious action," the "interconnected nature of cyberspace poses significant challenges for applying some of the legal frameworks developed for specific physical domains."[66]

Despite the difficulty of verifying the location from which an attack was launched or of identifying the attacker, DoD has announced it would

64. Draft Articles on Responsibility of States for Internationally Wrongful Acts, Rep. of the Int'l L. Comm'n, 53d Sess., UN GAOR 56th Sess., Supp. No. 10, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 26, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2), *available at* http://untreaty.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf [hereinafter Draft Rules of State Responsibility].

65. Sklerov, *supra* note 52, at 7.

66. Cyberspace Policy Report, *supra* note 13, at 8.

"actively [seek] to limit the ability of such potential actors to exploit or attack the United States anonymously."[67] It is, of course, almost commonplace to state that interagency and international cooperation, as well as information sharing, is a necessary prerequisite to achieve that goal. In view of the special characteristics of cyberspace, it may well be that international law provides an obligation to cooperate if States are prepared to take attribution measures in cyberspace. It will be interesting to see whether DoD's efforts to "assess the identity of the attacker via behavior-based algorithms" and to "significantly improve its cyber forensics capabilities"[68] are successful and, what is equally important, whether other States will accept the results as sufficient evidence of the source of a cyber attack.

E. Conclusions with Regard to Territorial Sovereignty

Territorial sovereignty has proven to be an effective principle of international law that can be applied to cyberspace without far-reaching modifications if cyberspace is understood as comprising components (cyber infrastructure) located in a State's territory or that are otherwise protected by the principle of territorial sovereignty. Of course, not all aspects of conduct constituting a violation of territorial sovereignty have been clarified. For instance, there is still no consensus among States as to which cyber operations qualify as a prohibited use of force under Article 2(4) of the UN Charter or as an armed attack under Article 51. Also, the rather abstract references to "critical infrastructure" as being protected by the principle of territorial sovereignty are not very helpful in the absence of a consensus as to which objects and governmental institutions are to be considered "critical" in nature.

The concept of territorial jurisdiction also provides an effective basis for the regulation of cyber activities. States are entitled to regulate activities occurring within their territories and to enforce their domestic law. Although States enjoy an almost unlimited right to exercise their jurisdiction over cyber activities and cyber infrastructure within their territory, there is an undisputable need for an internationally agreed understanding that the Internet's functionality—the benefits it provides—would be seriously challenged if States do not exercise their jurisdiction "with respect for one another's networks and the broader Internet."[69]

67. *Id.* at 4.
68. *Id.*
69. INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 13, at 10.

III. NEUTRALITY

"Neutrality" denotes the legal status of a State that is not a party to an international armed conflict. Since the rules of international law applicable to neutral States are predominantly laid down in 1907 Hague Conventions V[70] and XIII,[71] one might assume that the law of neutrality has become obsolete by desuetude or because an impartial stance vis-à-vis the aggressor and the victim of aggression would be irreconcilable with the *jus ad bellum* as codified in the UN Charter.

Indeed the international armed conflicts that have occurred since the end of the Second World War (e.g., the conflicts between Israel and Egypt, India and Pakistan, the United Kingdom and Argentina, and Iraq and Iran) might cast doubts on the continuing validity of the traditional law of neutrality. This does not establish, however, that there is no longer a law of neutrality. The very fact that some neutral governments have tried to conceal their "unneutral service" is in itself evidence those governments considered themselves bound by the law of neutrality. And those governments that openly supported one side of an international armed conflict—in most instances because the aggrieved belligerent was unable to react to their non-compliance with neutral obligations—often went to great length to justify their conduct.

States, although their conduct may not always have been in full compliance with the principle of impartiality, have, however, recognized that the traditional law of neutrality continues to apply in situations of international armed conflict.[72] The military manuals of the United States,[73] Canada,[74] the

70. Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310 [hereinafter Hague V].

71. Convention No. XIII Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415 [hereinafter Hague XIII].

72. *See* Dietrich Schindler, *Transformations in the Law of Neutrality since 1945*, *in* HUMANITARIAN LAW OF ARMED CONFLICT – CHALLENGES AHEAD, ESSAYS IN HONOUR OF FRITS KALSHOVEN 367 (Astrid J.M. Delissen & Gerard J. Tanja eds., 1991); Wolff Heintschel von Heinegg, *Wider die Mär vom Tode des Neutralitätsrechts*, *in* CRISIS MANAGEMENT AND HUMANITARIAN PROTECTION, FESTSCHRIFT FÜR DIETER FLECK 221 (Horst Fischer et al. eds., 2004).

73. U.S. Navy, U.S. Marine Corps & U.S. Coast Guard, NWP 1-14M/MCWP 5-12/COMDTPUB P5800.7A, The Commander's Handbook on the Law of Naval Operations ch. 7, (2007) [hereinafter Commander's Handbook].

74. OFFICE OF THE JUDGE ADVOCATE GENERAL, DEPARTMENT OF NATIONAL DEFENCE (CANADA), LAW OF ARMED CONFLICT AT THE OPERATIONAL AND TACTICAL LEVELS ch. 13 (2003).

United Kingdom[75] and Germany,[76] as well as the *San Remo Manual*,[77] the International Law Association's Helsinki Principles[78] and the *HPCR Manual*,[79] all address the continued applicability of the law of neutrality to international armed conflicts. Thus, both State practice and writings establish the law of neutrality is alive and well.[80]

Under the UN Charter it is, at least in theory, possible to distinguish between an aggressor and the victim of aggression. This does not mean that States are entitled to unilaterally absolve themselves from the obligations of the law of neutrality and take a "benevolent" attitude in favor of the alleged victim of an unlawful use of force.[81] If, however, the UN Security Council has decided upon preventive or enforcement measures under Chapter VII of the UN Charter, the scope of applicability of the law of neutrality will be reduced considerably and the 1907 Hague Conventions will be inapplicable.[82] Under Articles 25 and 103 of the UN Charter, States

---

75. UNITED KINGDOM MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT (2004). It is important to note that the *UK Manual* does not contain a chapter specifically devoted to the law of neutrality; however, its continuing validity is expressly recognized in paragraph 1.42, and chapters 12 (Air Operations) and 13 (Maritime Warfare) contain rules on neutral States, neutral aircraft and neutral vessels.

76. FEDERAL MINISTRY OF DEFENCE (GERMANY), HUMANITARIAN LAW IN ARMED CONFLICTS MANUAL ch. 11 (1992) [hereinafter GERMAN MANUAL].

77. SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA ¶¶ 7–26, 28–32, 34–36, 60, 67–71, 74–75, 85–88, 92–94, 106, 108–10, 113–16, 118–20, 122–27, 130, 132–35, 141, 146–47, 151–57, 161, 165–68, 179–83 (Louise Doswald-Beck ed., 1995).

78. Committee on Maritime Neutrality, International Law Association, *Helsinki Principles on the Law of Maritime Neutrality, May 30, 1998*, *in* INTERNATIONAL LAW ASSOCIATION, REPORT OF THE 68TH CONFERENCE TAIPEI, 1998, at 496 (1998), *reprinted in* THE LAWS OF ARMED CONFLICTS: A COLLECTION OF CONVENTIONS, RESOLUTIONS AND OTHER DOCUMENTS 1425 (Dietrich Schindler & Jiri Toman eds., 4th ed. 2004) [hereinafter Helsinki Principles].

79. HPCR MANUAL, *supra* note 26, sec. X.

80. *See* Heintschel von Heinegg, *supra* note 72, at 232.

81. Wolff Heintschel von Heinegg, *"Benevolent" Third States in International Armed Conflicts: The Myth of the Irrelevance of the Law of Neutrality*, *in* INTERNATIONAL LAW AND ARMED CONFLICT: EXPLORING THE FAULTLINES 543 (Michael N. Schmitt & Jelena Pejic eds., 2007).

82. *See* SAN REMO MANUAL, *supra* note 77, ¶¶ 7–9; HPCR MANUAL, *supra* note 26, rule 165; Helsinki Principles, *supra* note 78, ¶ 1.2. For the powers of the UN Security Council and the obligations of UN member States, see DINSTEIN, *supra* note 49, at 308–15. For a restrictive approach to the powers of the UN Security Council, see ERIKA DE WET, THE CHAPTER VII POWERS OF THE UNITED NATIONS SECURITY COUNCIL 133–74 (2004).

not parties to an international armed conflict are obliged to comply with UN Security Council decisions and, in any event, to refrain from activities interfering with or impeding the exercise of enforcement operations authorized by resolutions implementing those decisions.[83]

In view of the foregoing, this section starts from the premise that, subject to decisions by the UN Security Council under Chapter VII of the UN Charter, the traditional law of neutrality applies to States not parties to an international armed conflict. It will first explore whether, and to what extent, that body of law is applicable to cyberspace. It will then identify the obligations of belligerents and of neutrals with regard to military operations in cyberspace.

A. Applicability of the Law of Neutrality to Cyberspace

The continuing validity of the core principles and rules of the law of neutrality in an international armed conflict characterized by the use of traditional kinetic weapons is beyond question. But when it comes to hostilities and hostile acts conducted in or through cyberspace, some might reject their applicability. Indeed, if cyberspace is considered to be a new "fifth dimension," a "global common" that "defies measurement in any physical dimension or time space continuum,"[84] it could be rather difficult to maintain that the law of neutrality applies. If it is acknowledged, however, that cyberspace "requires a physical architecture to exist,"[85] many of the difficulties can be overcome.

The law of neutrality serves a dual protective purpose. On the one hand, it is to protect the territorial sovereignty of neutral States and their nationals against the harmful effects of the ongoing hostilities. On the other hand, it aims to protect belligerent interests against interference by neutral States and their nationals to the benefit of one belligerent and to the detriment of the other. Thus, the rules and principles of the law of neutrality aim to prevent escalation of an ongoing international armed conflict "[by] regulating the conduct of belligerents with respect to nations not participating in the conflict, [by] regulating the conduct of neutrals with re-

83. For an analysis of the effects of UN Charter Article 103, see Rudolf Bernhardt, *Article 103*, *in* 2 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 1292, 1295–1302 (Bruno Simma et al. eds., 2d ed. 2002).

84. WINGFIELD, *supra* note 6, at 17.

85. Franzese, supra note 8, at 33. *See also supra* notes 10–13 and accompanying text.

spect to belligerents, and [by] reducing the harmful effects of such hostilities on international commerce."[86]

Applied in the cyber context, it is safe to conclude that the law of neutrality protects the cyber infrastructure located in the territory of a neutral State or that resides in sovereign immune platforms and other objects used by the neutral State for non-commercial government purposes. Thus, belligerents are under an obligation to respect the sovereignty and inviolability of States not parties to the international armed conflict by refraining from any harmful interference with the cyber infrastructure located in neutral territory. Neutral States must remain impartial and may not engage in cyber activities that support the military actions of one belligerent to the detriment of the opposing belligerent. Moreover, they are obliged to take all feasible measures to terminate an abuse of the cyber infrastructure located within their territory or on their sovereign immune platforms by the belligerents.

Because they are based upon a teleological interpretation of the law of neutrality, some may question these findings; however, they are supported not only by the majority of authors addressing the issue of neutrality in the cyber context,[87] but also by State practice. For instance, DoD has taken the position that "long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace."[88] DoD's Cyberspace Policy Report, *inter alia*, emphasizes that "applying the tenets of the law of armed conflict [is] critical."[89] The report also addresses activities "taking place on or through computers or other infrastructure located in a neutral third country."[90] The applicability of the law of neutrality to cyberspace has also been acknowledged in the recent *HPCR Manual*.[91] Since that manual has been endorsed by a considerable number of governments, it may be considered a restatement of the existing law, and as reflecting the consensus of those States on the issues it addresses.

Of course, the rules of the traditional law of neutrality, while in principle applicable to cyberspace, may require clarification—or even modifica-

86. Commander's Handbook, *supra* note 73, ¶ 7.1.

87. *See, e.g.*, Kastenberg, *supra* note 12, at 56–64; Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 AIR FORCE LAW REVIEW 65, 90–91 (2009); George K. Walker, *Information Warfare and Neutrality*, 33 VANDERBILT JOURNAL OF TRANSNATIONAL LAW, 1079, 1182–84 (2000).

88. DoD Strategy for Operating in Cyberspace, *supra* note 9, at 9.

89. Cyberspace Policy Report, *supra* note 13, at 8.

90. *Id.*

91. HPCR MANUAL, *supra* note 26, rule 168(b).

tion—because of the unique characteristics of cyberspace.[92] Still the "law of armed conflict and customary international law . . . provide a strong basis to apply such norms to cyberspace governing responsible state behavior."[93]

B. Obligations of Belligerents

Under the law of neutrality belligerents are obliged to respect the inviolability of neutral territory; hence, they are prohibited from conducting hostilities, from exercising belligerent rights or establishing bases of operations within neutral territory. These prohibitions are laid down in international treaties[94] and they are considered customary in character.[95]

1. No Harmful Interference with Neutral Cyber Infrastructure

It follows from the foregoing that cyber infrastructure located within the territory of a neutral State is protected against harmful interference by the belligerents. It does not matter whether the cyber infrastructure is owned or exclusively used by the government, corporations or private individuals. Neither does the protection depend upon the nationality of the owner. In view of the principle of sovereign immunity, the same protection applies to cyber infrastructure located on neutral State ships and State aircraft or in diplomatic premises.

The prohibition on harmful interference with neutral cyber infrastructure is not limited to cyber attacks *strictu sensu*, i.e., to cyber operations that cause, or are expected to cause, damage, destruction, death or injury. Rather, it is to be understood as also comprising all activities, whether kinetic or cyber, that either have a negative impact on their functionality or make their use impossible. In other words, it is prohibited to engage in "the use of network-based capabilities . . . to disrupt, deny, degrade, manipulate, or

92. Cyberspace Policy Report, *supra* note 13, at 7.

93. *Id.* at 8.

94. Hague V, *supra* note 70, arts. 1–3; Hague XIII, *supra* note 71, arts. 1–2, 5.

95. *See* Commander's Handbook, *supra* note 73, ¶ 7.3; GERMAN MANUAL, *supra* note 76, ¶¶ 1108, 1149; SAN REMO MANUAL, *supra* note 77, ¶ 15; HPCR MANUAL, *supra* note 26, rule 166. *See also* Hague Rules of Aerial Warfare arts. 39, 40, 42, 47, Feb. 19, 1923, 32 AMERICAN JOURNAL OF INTERNATIONAL LAW SUPPLEMENT 12 (1938) (not in force), *reprinted in* THE LAWS OF ARMED CONFLICTS, *supra* note 78, at 315 [hereinafter 1923 Hague Air Rules].

destroy information resident in computers and computer networks, or the computers and networks themselves"[96] of a neutral State.

Of course, as previously noted, mere intrusion into neutral cyber infrastructure is not covered by this prohibition, because international law does not prohibit espionage. It must be borne in mind, however, that the principle of territorial sovereignty includes the prohibition on exercising jurisdiction on foreign territory;[97] therefore a cyber operation characterized as an exercise of jurisdiction would be in violation of the sovereignty of the target State. That prohibition is of a general character and thus not part of the law of neutrality *strictu sensu*.

2. Exercise of Belligerent Rights and Use of Cyber Infrastructure in Neutral Territory

Belligerents are prohibited from using neutral cyber infrastructure for the purpose of exercising belligerent rights against the enemy or against others. It is important to note that the term "belligerent rights" is not limited to cyber attacks, but refers to all measures a belligerent is entitled to take under the law of armed conflict against the enemy belligerent, enemy nationals or the nationals of neutral States.[98] This prohibition follows from the very object and purpose of the law of neutrality, i.e., to prevent an escalation of the international armed conflict.

In view of its object and purpose, this prohibition also applies to the exercise of belligerent rights through the use of neutral cyber infrastructure that enjoys sovereign immunity, that is, infrastructure located outside neutral territory used by a neutral State for exclusively non-commercial government purposes. It is not as certain that the prohibition also applies to the use of cyber infrastructure owned by a private corporation or an individual located outside neutral territory. In such a situation, however, the cyber infrastructure can be considered as contributing to the enemy's mili-

96. Schaap, *supra* note 5, at 127.

97. *Lotus, supra* note 1, at 18–19 ("Now the first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.").

98. Such actions comprise detention, requisitions, capture and interception.

tary action and the opposing belligerent would be entitled to treat it as a lawful military objective.[99]

Moreover, a belligerent may not make use of its own cyber infrastructure for military purposes if it is located on neutral territory. It is irrelevant whether the cyber infrastructure has been "erected" prior to or after the outbreak of the international armed conflict. This prohibition follows from Article 3 of Hague V, according to which

> belligerents are . . . forbidden to:
>
> (a) Erect on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea;
>
> (b) Use any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the purpose of public messages.

3. Exceptions to the Prohibition on Exercising Belligerent Rights

As has been discussed, the prohibition on exercising belligerent rights through the use of neutral cyber infrastructure must be interpreted in the light of the unique characteristics of cyberspace.[100] Cyberspace is an "interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[101] Given the interdependence and ubiquity of cyberspace and its components, it would be almost impossible for a belligerent to prevent the routing of malicious data packages through the cyber infrastructure located in the territory of a neutral State even though it is ultimately aimed against the enemy. Therefore, it seems to be

---

99. For the definition of lawful military objectives, see Article 52(2) of the 1977 Additional Protocol I to the 1949 Geneva Conventions. This definition reflects customary international law. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3.

100. *See supra* note 84 and accompanying text.

101. Dictionary of Military and Associated Terms, *supra* note 5. See also the definition by Schaap, *supra* note 5, at 126 ("cyberspace" is a "domain characterized by the use of [computers and other electronic devices] to store, modify, and exchange data via networked systems and associated physical infrastructures").

logical and perhaps even cogent to apply Article 8 of Hague V to cyber operations and cyber attacks conducted by a belligerent against its enemy. Article 8 provides: "A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."

Doubts have been articulated in the literature as to whether Article 8 has any application to cyberspace.[102] That position is based on the assumption that a cyber operation conducted through neutral cyber infrastructure is to be considered as originating from neutral territory. Article 8, however, only applies to communications. It is Article 2 of Hague V that prohibits belligerents, *inter alia*, from moving "munitions of war or supplies across the territory of a neutral Power." If the distinction between mere communications through and passage of "munitions of war . . . across" were applied to cyberspace, any transmission of a cyber weapon through neutral cyber infrastructure would constitute a violation of the law of neutrality, whereas mere communications would not. Indeed, there are some indications that States share that view. For instance, in 1999 DoD's Office of General Counsel arrived at the conclusion that "[t]here is nothing in this agreement [i.e., Hague V] that would suggest that it applies to systems that generate information, rather than merely relay communications."[103] It is interesting to note that DoD seems prepared to apply Article 8 to cyberspace, although it would limit its applicability to mere communications, i.e., to cyber operations that do not amount to a cyber attack.

Articles 2 and 8 of Hague V are based on the assumption that a neutral State exercises full and effective control over its entire territory, but not over installations and objects used for communications purposes. The different degrees of feasible and effective control must also be taken into account in the cyber context. In recognition of the nature of cyberspace, the *HPCR Manual* provides: "[W]hen Belligerent Parties use for military purposes a public, internationally and openly accessible network such as the Internet, the fact that part of this infrastructure is situated within the jurisdiction of a Neutral does not constitute a violation of neutrality."[104]

---

102. Kastenberg, *supra* note 12, at 56–64; Todd, *supra* note 87, at 90–91.

103. Office of General Counsel, U.S. Department of Defense, An Assessment of International Legal Issues in Information Operations 10 (May 1999), *available at* http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf.

104. HPCR MANUAL, *supra* note 26, rule 167(b).

The *HPCR Manual* does not distinguish between mere communications on the one hand and the transmission of cyber weapons on the other. The phrase "use for military purposes" is sufficiently broad to cover both. This seems to be a reasonable adaptation of the traditional rules of the law of neutrality to cyberspace. Because of the complexity and interdependence of contemporary networks, such as the Internet, it is impossible to exercise the control necessary to effectively interfere with communications over such networks. This is underlined by the fact that most such communications are often neither traceable nor predictable since they will be transmitted over lines of communications and routers passing through various countries before reaching their ultimate destinations. These realities being taken into account, under this view, the mere fact that military communications, including cyber attacks, have been transmitted via the cyber infrastructure of a neutral State is not considered to constitute a violation of that State's neutral obligations.

It is acknowledged, despite the attractiveness of the *HPCR Manual*'s approach for both belligerents and neutral States, it is unclear that such a far-reaching adaptation of Article 8 to cyber operations conducted for military purposes will ultimately be accepted as reflective of contemporary customary international law. Modern State practice, especially the cyber operations during the 1999 Kosovo campaign, the conflicts in Afghanistan (2001) and Iraq (2003), and the armed conflict between Georgia and Russia (2007), provides insufficient evidence to establish that a cyber operation, including the transmission of cyber weapons through neutral cyber infrastructure, does not violate the neutrality of the States through which the transmissions passed. First, there is no open-source information establishing that the cyber operations amounted to cyber attacks or that they had been routed through neutral cyber infrastructure. Second, the distributed denial-of-serve attacks against Georgia, according to the position taken by this author, do not qualify as cyber attacks *strictu sensu* and, therefore, cannot be assimilated to the transit of "munitions of war" under Article 2 of Hague V. On the other hand, the DoD's Cyberspace Policy Report suggests the United States considers every "malicious cyber activity" as a violation of the law of neutrality, irrespective of whether they have been launched from or merely transmitted through "computers or other infrastructure located in a neutral third country."[105]

105. Cyberspace Policy Report, *supra* note 13, at 8.

What is clear today is that the use of neutral cyber communications by a belligerent does not constitute a violation of neutrality even though it serves military purposes. It is less clear, however, that this is also true if the cyber operation qualifies as a "malicious cyber activity" or cyber attack. We will return to this issue in the context of the consequences of a violation of the law of neutrality by neutral States.

C. Obligations of Neutral States

The law of neutrality, in view of its object and purpose,[106] poses obligations not only upon the belligerents, but also on neutral States. Setting aside the duty of impartiality,[107] a neutral State's obligations may be divided into three categories: (1) a prohibition on allowing or tolerating the exercise of belligerent rights in its territory, (2) an obligation to terminate (and probably to prevent) a violation of its neutrality by a belligerent and (3) an obligation to accept the enforcement of the law of neutrality by the aggrieved belligerent.

1. The Prohibition on Allowing or Tolerating the Exercise of Belligerent Rights

According to Article 5 of Hague V, a "neutral Power must not allow any of the acts referred to in Articles 2 to 4 to occur in its territory." Accordingly, a neutral State may not allow or tolerate the exercise of belligerent rights that utilize either the cyber infrastructure located within its territory or that located outside its territory, provided that the neutral State exercises exclusive control over it.[108]

The different interpretations of Article 8 of Hague V may have far-reaching consequences. Under the *HPCR Manual* approach,[109] a malicious cyber activity routed through neutral cyber infrastructure that is, for example, a component of the Internet would not constitute a prohibited exercise

106. *See supra* note 86 and accompanying text.

107. Hague V, *supra* note 70, art. 9. Article 9 of Hague XIII provides a "neutral Power must apply impartially to the two belligerents the conditions, restrictions, or prohibitions made by it." Accordingly, restrictions on military communications via its cyber infrastructure must be applied impartially by the neutral State. *See also* SAN REMO MANUAL, *supra* note 77, ¶ 19.

108. *See supra* notes 98–105 and accompanying text.

109. HPCR MANUAL, *supra* note 26, rule 167(b).

of belligerent rights. Therefore, a neutral State allowing or tolerating such an activity would not violate its obligations under the law of neutrality. If, however, the *HPCR Manual* approach is not considered to reflect customary international law, the transmission of a cyber attack through neutral infrastructure would have to be considered a prohibited exercise of belligerent rights, and the neutral State that knowingly allows or tolerates the transmission would be in violation of its neutral obligations.

But even if the latter approach is taken, the consequences are less grave than one may assume. Contrary to the position of one author,[110] the use of the term "allow" in the traditional rule presupposes knowledge by the neutral State. That will be the case if it has detected a malicious cyber activity/cyber attack or if it has been informed in a sufficiently credible manner that the activity/attack has originated from, or has been transmitted through, the State's cyber infrastructure. Such knowledge will result in a violation of the law of neutrality by the neutral State only if the malicious cyber activity continues. In most cases, cyber attacks will occur at such high speed that the knowledge that it has occurred is available only after the event. *Ex post facto* knowledge hardly suffices to justify a claim of a violation of the law of neutrality.

Even if constructive—as opposed to actual—knowledge is considered sufficient to establish a violation of the obligation that too would not result in noticeable changes in the manner in which the law of neutrality applies. Constructive knowledge means that the neutral State should have known of the malicious activity, but, again, in most cases such knowledge would not necessarily result in a violation of neutral obligations, because of the speed of cyber operations.

The analysis would probably be different if, as a result of the prohibition of allowing the exercise of belligerent rights, neutral States were obliged to actively monitor cyber activities originating from or transiting through their cyber infrastructure; however, it is far from settled that such an obligation exists. The *San Remo Manual*, in addressing physical violations of neutral territory, provides that a "neutral State must take such measures . . . including the exercise of surveillance, as the means at its disposal allow, to prevent the violation of its neutrality by belligerent forces."[111] It is not likely, however, that States, especially those that defend the freedom of Internet communications, will agree that the obligation to monitor land areas

110. Kastenberg, *supra* note 12, at 57.

111. SAN REMO MANUAL, *supra* note 77, ¶ 15.

and certain sea areas applies equally to the cyber infrastructure located in their territory.

2. Obligation to Terminate and to Prevent a Violation of Neutrality

According to the traditional law of neutrality, neutral States are obliged to terminate an exercise of belligerent rights and any other violation of their neutrality by one of the belligerents.[112] This obligation is part of contemporary customary international law.[113]

The obligation to enforce neutral status against violations by the belligerents is not absolute in character, but is limited to what is feasible. In other words, the neutral State is obliged to use all means reasonably available to it to terminate an exercise of belligerent rights occurring within its territory.[114] The applicable standard is not objective but rather subjective; it depends on the means and capabilities factually available to the neutral State. It must be emphasized that, subject to feasibility, the duty to enforce neutral status entails an obligation to use all means necessary, including the use of force, to effectively terminate an unlawful exercise of belligerent rights. The belligerent against which such measures are applied may not consider them as a hostile act, that is, it is obliged to tolerate them as a lawful action by the neutral State carrying out its neutrality obligations.[115]

The obligation to terminate an ongoing violation of neutrality presupposes knowledge—actual or constructive—by the neutral State.[116] It is quite probable that the neutral State is unaware of an abuse of its cyber infrastructure. But even if such actual or constructive knowledge existed, it would in most cases be futile to demand the neutral State take measures against the belligerent, because the cyber operation triggering the duty to terminate has been completed.

---

112. *Id.*, ¶¶ 18, 22; HPCR MANUAL, *supra* note 26, rule 168(a). *See also* 1923 Hague Rules, *supra* note 95, arts. 42, 47.

113. SAN REMO MANUAL, *supra* note 77, ¶ 22; HPCR MANUAL, *supra* note 26, rule 168(a); Commander's Handbook, *supra* note 73, ¶ 7.3; GERMAN MANUAL, *supra* note 76, ¶ 1109.

114. SAN REMO MANUAL, *supra* note 77, ¶ 22; HPCR MANUAL, *supra* note 26, rule 168(a); Commander's Handbook, *supra* note 73, ¶ 7.3; GERMAN MANUAL, *supra* note 76, ¶ 1109.

115. Hague V, *supra* note 70, art. 10; HPCR MANUAL, *supra* note 26, rule 169; 1923 Hague Air Rules, *supra* note 95, art. 48.

116. *See supra* note 104 and accompanying text.

Limiting a neutral's obligation to the termination of ongoing cyber activities is considered by some authors to be insufficient. They assert that a neutral State is also obliged to take all feasible measures to prevent an exercise of belligerent rights, that is, to act before it occurs.[117] At first glance, that position seems to reflect customary international law, because some military manuals expressly refer not only to an obligation to terminate an ongoing violation of neutrality, but also to a duty to prevent an exercise of belligerent rights within neutral territory.[118] It is, however, doubtful whether the use of the term "prevent" is meant to establish an obligation vis-à-vis future violations of neutrality. But even if that were the case, the duty to prevent would be limited to violations of neutral territory and national airspace. It is far from clear that States are willing to accept a prevention requirement, because that implies an obligation to continuously monitor cyber activities originating from or transiting through their cyber infrastructure. Additionally, monitoring would be of limited utility since, as has been shown, the identification of the malicious nature of data packages transiting through a network would in most cases be extremely difficult, if not impossible.

Therefore, there are good reasons for rejecting a prospective duty of prevention. If there is such an obligation, it exists only with regard to activities within neutral territory that could be assimilated to those covered by Article 8 of Hague XIII.[119] For instance, the authorities of a neutral State may have actual or constructive knowledge of the activities of a group of hackers that has been employed by a belligerent government to develop a cyber weapon to be used against the enemy. In such a situation the neutral State would be obliged to take all feasible measure to prevent the departure of the cyber weapon from its territory.

---

117. Kastenberg, *supra* note 12, at 56–64.

118. SAN REMO MANUAL, *supra* note 77, ¶ 15; HPCR MANUAL, *supra* note 26, rule 168(a); Commander's Handbook, *supra* note 73, ¶ 7.3.

119. A neutral Government is bound to employ the means at its disposal to prevent the fitting out or arming of any vessel within its jurisdiction which it has reason to believe is intended to cruise, or engage in hostile operations, against a Power with which that Government is at peace. It is also bound to display the same vigilance to prevent the departure from its jurisdiction of any vessel intended to cruise, or engage in hostile operations, which had adapted entirely or partly within the said jurisdiction for use in war.

3. Consequences of Non-compliance by Neutral States

The law of neutrality provides that if a neutral State fails to terminate an exercise of belligerent rights or other violations of its neutrality by one belligerent, the other belligerent is entitled to take those measures necessary to terminate the violation.[120] The right of the aggrieved belligerent to enforce the law of neutrality comes into operation if the neutral State is either unwilling or unable to comply with its obligation to terminate a violation of its neutral status by the enemy. This right is a specific form of a countermeasure, i.e., a measure that would be unlawful if it was not taken in response to a violation of international obligations by the target State.[121] Its object and purpose are (1) to induce the neutral State to comply with its obligations and (2) to enable the aggrieved belligerent to preserve its security interests. Not every violation of neutrality by one belligerent justifies a resort to countermeasures by the other belligerent. The violation in question must have a negative impact on the legitimate security interests of that belligerent. This will not be the case if a belligerent takes measures against a neutral State's cyber infrastructure that do not provide a military advantage vis-à-vis the other belligerent. In that case, the right to respond to the violation is reserved to the neutral State and the exercise of that right is probably subject to a *de minimis* exception.

When the neutral State does not act to terminate a violation of its neutrality, the aggrieved belligerent is not entitled to immediately resort to the exercise of countermeasures. In that regard, the *San Remo Manual* provides: "If the neutral State fails to terminate the violation of its neutral waters by a belligerent, the opposing belligerent must so notify the neutral State and give that neutral State a reasonable time to terminate the violation by the belligerent."[122] An immediate response by the aggrieved belligerent is lawful only if (1) the violation constitutes a serious and immediate threat to the security of that belligerent, (2) there is no feasible and timely alternative and (3) the enforcement measure taken is necessary to respond to the threat posed by the violation.[123]

---

120. Commander's Handbook, *supra* note 73, ¶ 7.3; SAN REMO MANUAL, *supra* note 77, ¶ 22; HPCR MANUAL, *supra* note 26, rule 168(b). For those who believe there is also an obligation to prevent a violation, the other belligerent would also have the right to act if the neutral State fails to do so.

121. *See* Draft Articles on State Responsibility, *supra* note 64, arts. 22, 49–54.

122. SAN REMO MANUAL, *supra* note 77, ¶ 22.

123. *Id. See also* HPCR MANUAL, *supra* note 26, rule 168(b).

The aggrieved belligerent's right to enforce the law of neutrality certainly applies to cyberspace if a malicious cyber activity originates from the territory of a neutral State.[124] DoD seems to be prepared to take such enforcement measures if it is determined a neutral State is aware of the malicious cyber activity. The Cyberspace Policy Report indicates that in making that determination the following will be taken into account:

> The nature of the malicious cyber activity; the role, if any, of the third country; the ability and willingness of the third country to respond effectively to the malicious cyber activity; and the appropriate course of action for the U.S. Government to address potential issues of third-party sovereignty depending upon the particular circumstances.[125]

This is a clear restatement of the rules of the law of neutrality, providing evidence of DoD's willingness to apply those rules to conduct in cyberspace.

D. Conclusions with Regard to the Law of Neutrality

It has been shown that the traditional law of neutrality is, in principle, applicable to cyberspace. This is especially true of belligerent cyber operations that qualify as an exercise of belligerent rights within neutral territory. As with the principle of territorial sovereignty, the special characteristics of cyberspace do not, as such, pose an obstacle to the application of that law. Certainly, however, there remains an urgent need for clarification and even adaptation of the traditional law. In view of the interdependence of the networks through which data are transmitted and the potentially disastrous effects on critical infrastructure subjected to a cyber attack, there is a high probability that belligerent States will take measures, including the use of kinetic force, against neutral States and their cyber infrastructure if they determine vital security interests are at stake. Such measures have the potential to jeopardize the essential object and purpose of the law of neutrality—preventing escalation of an international armed conflict.

---

124. *See* Cyberspace Policy Report, *supra* note 13, at 8.
125. *Id.*

IV. FINAL THOUGHTS

The U.S. government has taken helpful first steps in the identification of the applicable rules of international law and their interpretation in the context of the challenges brought about by the specific characteristics of cyberspace. Other governments should closely cooperate in a continuing effort to arrive at an operable consensus that takes into consideration global interoperability, network stability, reliable access and cybersecurity due diligence.[126] The five criteria identified in the International Strategy for Cyberspace should be accepted by other States because they are of a potentially norm-creating character and assist in clarifying the scope of existing rules and principles of international law applicable to the cyber domain. Moreover, governments should cooperate with a view to improving their capabilities in the area of cyber forensics. Such cooperative efforts are necessary not only in order to identify attackers, but also to establish a more effective deterrent of malevolent States and non-State actors.

126. INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 13, at 10.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

The Role of Counterterrorism Law in Shaping *ad Bellum* Norms for Cyber Warfare

William Banks

89 INT'L L. STUD. 157 (2013)

Volume 89 2013

The Role of Counterterrorism Law in Shaping *ad Bellum* Norms for Cyber Warfare

William Banks[*]

I. INTRODUCTION

Assume that senior government ministers meeting to discuss economic policies at the capital in a major industrial State are interrupted by an assistant who reports that large-scale malware programs have infected the critical infrastructure of the State and its private sector. In the security sector, large-scale routers throughout the network are failing, and classified systems have been penetrated. As the ministerial meeting suddenly shifts its attention to the fast-spreading cyber intrusion, the malware continues to spread, causing Internet-based systems to fail throughout the country. Government and financial institutions continue to be besieged by a distributed denial-of-service attack from tens of thousands of computers organized into botnets, a slang term for the tool that enslaves the computers of unknowing victims. Banks are forced to shut down, incoming payments due from abroad cannot arrive and government ministries close up shop. Credit card companies shut down their networks worldwide, fearing the

[*] Board of Advisors Distinguished Professor of Law; Director, Institute for National Security and Counterterrorism; Professor of Public Administration and International Affairs, Syracuse University. The author is grateful to Eric Jensen and Matthew Waxman for helpful comments on a draft version, and to Erin Lafayette and Egon Donnarumma for excellent research assistance.

spread of the attacks. Meanwhile, the national government closes all its electronic borders. There was as yet no physical damage and no deaths or injuries attributable to the cyber attacks, but the economic and social costs are high and mounting.

As the government's security, intelligence and law enforcement resources scramble to identify the source of the attacks and implement defensive measures, legal advisers face their own challenges. The first intelligence reports show the sources of the attack coming from computers all over the world, but with no clear indications of any State sponsorship or involvement. Meanwhile, terrorist groups opposed to certain of the victim-State government's policies have threatened attacks, but as yet the attacks cannot be clearly attributed. What body of law applies in responding to the attacks? Is the nation at war? If so, who is the enemy? Has there been a "use of force" or "armed attack" sufficient to trigger self-defense prerogatives under the UN Charter? Do the attacks create an "armed conflict" between the State and the unidentified enemy and, if so, do the laws of armed conflict (LOAC) apply? What is the source of the legal authority to respond defensively if the perpetrators are non-State terrorists? If the computers responsible for spreading the malware can be identified, but at this time not the State or non-State group perpetrating the attacks, what is the nature and scope of the authority to respond?

The prospect of cyber war has evolved from science fiction and over-the-top doomsday depictions on television, films and in novels to reality and front-page news. The revelations that the Stuxnet attack on the computers that run Iran's nuclear enrichment program was part of a larger "Olympic Games" campaign of cyber war begun in 2006 during the George W. Bush administration by the United States, and perhaps Israel, opened our eyes to the practical reality that the United States is engaged in some kind of cyber war against Iran. The United States' use of cyber weapons to attack a State's infrastructure became the first known use of computer code to effect physical destruction of equipment—in this case Iranian centrifuges—instead of disabling computers or stealing data.[1] If the United States can so target Iran's nuclear program, why not go after the North Koreans? Or the Assad regime in Syria, the Chinese military, or al

1. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES, June 1, 2012, at A1, *available at* http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all; *see also* DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER (2012).

Qaeda's global operations? If the United States can achieve important national security and foreign policy objectives through the use of cyber weapons, can there be any doubt that the United States is now the target of the same kinds of weapons?

Most computer attacks temporarily disable the computer or its applications, or exploit the computer by reporting back data to a remote host. More sophisticated intrusions, however, can cause more significant disruptions or even destruction, like the Iranian centrifuges or worse. Because our societies now entrust so much of our critical infrastructure to online systems, experts such as former Clinton and Bush administration cyber and counterterrorism adviser Richard A. Clarke warn that cyber attackers could derail trains, cause power blackouts, cause oil or gas pipelines to explode, or ground aircraft.[2]

Whether large or small, cyber attacks are proliferating, at least in part because the means are becoming cheaper and easier to acquire and use.[3] Particularly when targeted at powerful adversaries like the United States, cyber intrusions offer a model application of asymmetric warfare, where adversaries much weaker in conventional terms exploit vulnerabilities in the stronger foe. The asymmetric attackers are further advantaged by the fact that they may mask their identity and location at least temporarily and avoid immediate attribution and response to the attacks. As such, cyber attacks share core characteristics with other terrorist attack modes. As the means to affect cyber attacks become easier to acquire and use, terrorists may wage cyber war against their adversaries, either directly attacking government systems or going after infrastructure in the private sector.

Relatively little has been written about the legal bases for countering cyber terrorism,[4] and it has yet to be considered whether counterterrorism law could illuminate *ad bellum* norms for responding to cyber attacks perpetrated by terrorists or where the source of an attack cannot be promptly attributed and terrorists are suspected. The relative lack of attention given by States and international law experts to counterterrorism law as a source of authority to govern responses to cyber attacks is not surprising in view

2. RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 64–68 (2010).

3. *See id.*; JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 154 (2011).

4. Aviv Cohen, *Cyberterrorism: Are We Legally Ready?*, 9 JOURNAL OF INTERNATIONAL BUSINESS AND LAW 1 (2010); Irving Lachow, *Cyber Terrorism: Menace or Myth?*, *in* CYBERPOWER AND NATIONAL SECURITY 437, 448–49 (Franklin D. Kramer et al. eds., 2009).

of the difficulties more generally in the international community to identify and agree upon a legal paradigm for counterterrorism.[5] Although the international community continues to struggle to find an acceptable definition of terrorism,[6] it is generally understood that a cyber terrorist "uses Internet-based attacks in terrorist activities, including acts of deliberate, large-scale disruption of computer networks."[7] Like terrorism generally, cyber terrorism intends "to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological. . . . Attacks that lead to death or bodily injury, extended power outages, plane crashes, water contamination, or major economic losses would be examples."[8]

Meanwhile, the prospects for the use of cyber weapons by and against terrorist groups are increasing. Research conducted in the period immediately after the 9/11 attacks suggested that, although terrorists' interest in cyber attacks was increasing, their capabilities then were demonstrated only for theft and low-level attacks.[9] By implication, more disruptive or damaging versions of cyber terrorism could become a significant threat in the future. Meanwhile, at least since 2008 reports document likely Western government uses of cyber weapons against terrorist websites,[10] and U.S. use of cyber intrusions aimed at cell phone communications among terrorist leaders that could lure them to an ambush, spread false information that fellow jihadists were conspiring against their comrades and otherwise incite distrust of their supposedly secure communications.[11]

Even as experts recognize that terrorists may engage in cyber war, the international community continues to rely on a legal conception that limits

---

5. *See, e.g.*, Rosalyn Higgins, *The General International Law of Terrorism*, *in* TERRORISM AND INTERNATIONAL LAW 13, 13–14 (Rosalyn Higgins & Maurice Flory eds., 1997) ("terrorism is not a discrete topic of international law with its own substantive legal norms"); IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 745 (7th ed. 2008) ("There is no category of the 'law of terrorism' and the problems must be characterized in accordance with the applicable sectors of public international law . . . .").

6. STEPHEN DYCUS ET AL., COUNTERTERRORISM LAW 5–6 (2d ed. 2012).

7. SANDIA NATIONAL LABS., CYBER THREAT METRICS 11 n.4 (Sandia Report SAND2012-2427, Mar. 2012), *available at* http://prod.sandia.gov/techlib/access-control.cgi/2012/122427.pdf.

8. Dorothy E. Denning, *Is Cyber Terrorism Next?, in* UNDERSTANDING SEPTEMBER 11, at 193 (Craig Calhoun, Paul Price & Ashley Timmer eds., 2002).

9. *Id.* at 135–36; *see also* Lachow, *supra* note 4.

10. *See, e.g.*, Ian Black, *Cyber-attack theory as al-Qaida websites close*, GUARDIAN, Oct. 22, 2008, International Pages, at 16.

11. Eric Schmitt & Thom Shanker, *After 9/11, an Era of Tinker, Tailor, Jihadist, Spy*, NEW YORK TIMES, Aug. 7, 2011, § SR, at 6.

terrorism to "acts of violence committed in time of peace,"[12] a categorization that excludes most, though not all, cyber attacks. Despite the growing role of the cyber domain in the security sectors of many governments over the last decade, the maturing legal architecture for cyber war pays little attention to cyber attacks by terrorists or to cyber attacks that do not produce harmful effects equivalent to kinetic attacks. A distinguished International Group of Experts was invited by NATO in 2009 to produce a manual on the law governing cyber warfare.[13] The resulting *Tallinn Manual on the International Law Applicable to Cyber Warfare* restates the consensus view that prohibits "cyber attacks, or the threat thereof, the primary purpose of which is to spread terror among the civilian population."[14] The *Tallinn Manual* experts concluded that cyber attacks can constitute terrorism, but only where the attack has been conducted through "acts of violence."[15] In defining the scope of their project, the *Tallinn Manual* experts considered only those forms of cyber attack that meet the UN Charter and LOAC conceptions of "use of force" or "armed attack."[16] In other words, the *Tallinn Manual* concludes that international law proscribes only violent terrorism and thus leaves unregulated an entire range of very disruptive cyber intrusions.[17] To date there has been little attention given to the possibility that international law generally and counterterrorism law in particular could and should develop a subset of cyber-counterterrorism law to respond to the inevitability of cyber attacks by terrorists and the use of cyber weapons by governments against terrorists, and to supplement existing international law governing cyber war where the intrusions do not meet the traditional kinetic thresholds.

Developing a consensus understanding of the international law of cyber war is complicated by a few unique attributes of the cyber domain. Prompt attribution of an attack and even threat identification can be very difficult. As a result, setting the critical normative starting point in the UN

12. Jelena Pejic, *Armed Conflict and Terrorism: There Is a (Big) Difference*, *in* COUNTER-TERRORISM: INTERNATIONAL LAW AND PRACTICE 203 (Ana Maria Salinas de Frías, Katja L.H. Samuel & Nigel D. White eds., 2012).

13. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

14. *Id.*, rule 36.

15. *Id.*, rule 36, cmt. 2; rule 30.

16. *Id.* at 18.

17. *Id.*, rule 30, cmt. 12 (the majority of the International Group of Experts concluded that cyber intrusions that cause large-scale adverse consequences throughout the State but no physical damage do not trigger LOAC rules).

Charter and laws of armed conflict—the line between offense and defense—is elusive, particularly taking into account the possibilities afforded by cyber "active defenses." Is it lawful to anticipate cyber attacks by implementing countermeasures in advance of the intrusion? How disruptive or destructive a response does the law permit once a source of the incoming intrusions is identified, even plausibly? If victim States cannot reliably attribute incoming attacks, must they delay all but the most passive responses until the threat can be reliably identified? In addition, because cyber attacks will likely originate from multiple sources in many States, using geography as a proxy for a battlespace may not be realistic or useful in the cyber context. Even assuming attribution of incoming attacks, which, if any, geographic borders should define the scope of a victim State's responses?

Even with these limitations, there may be emerging legal clarity in some cyber war situations. In instances where a cyber attack causes physical destruction and/or casualties at a significant level, a cyber intrusion may constitute an "armed attack" in UN Charter terms. In these extreme circumstances, even where the attacker is a State-sponsored non-State actor, there is emerging post–September 11 customary law permitting a forceful response in self-defense, assuming attribution of the attacker.[18] In addition, whether the Charter criteria have been met is most likely a function of the consequences of the cyber event, and is not dependent on the instrument used in the attack.[19] Apart from this relatively small subset of cyber intrusions, however, the legal regime remains clouded and ambiguous.

International law scholars and operational lawyers have struggled over the last decade to accommodate LOAC and the UN Charter system to asymmetric warfare waged by non-State actors, including terrorist groups. A similar effort is now under way—evidenced by the *Tallinn Manual* project—to incorporate cyber war in our long-standing positive law systems for protecting civilians from the ravages of war. Yet the language and structure of LOAC (the regulation of "armed conflict") and of the Charter (focusing on "use of force" and "armed attack") present considerable analytic challenges and even incongruities in attempting to fit cyber into the conventional framework for armed conflict. Because cyber attacks may occur continuously or in stages with no overt hostility and range from low-level harassment to potentially catastrophic harms to a State's infrastructure, the

18. *Id.*, rule 13.

19. TALLINN MANUAL, rule 11–12.

either/or dichotomies of war and peace and armed conflict/no armed conflict are not in most instances well suited to the cyber domain. Nor are the Charter threshold requirements—that there be suffered by a victim State a "use of force" or "armed attack" before forceful defenses are employed—easily interpreted to accommodate cyber attacks. Over time, the ongoing struggle to fit cyber into the LOAC and Charter categories may threaten their normative integrity and their basic commitment to collective security and restraints on unilateral uses of force.

Most cyber intrusions now and in the foreseeable future will take place outside the traditional consensus normative framework for uses of force supplied by international law. For the myriad, multilayered and multifaceted cyber attacks that disrupt but do not destroy, whether State-sponsored or perpetrated by organized private groups or single hacktivists, much work remains to be done to build a normative architecture that will set enforceable limits on cyber intrusions and provide guidelines for responses to disruptive cyber intrusions. In this article, my interest is directed at a subset of those cyber attacks—those where terrorists are responsible or attribution is not known but points in the terrorists' direction, and where the effects are very disruptive but not sufficiently destructive to cross the traditional LOAC and Charter self-defense thresholds.

For this subset of cyber attacks, counterterrorism law may offer a useful complementary normative supplement to LOAC and the Charter. Especially over the last decade, a corpus of counterterrorism law has evolved as domestic and international law in response to transnational terrorism. In contrast to the dominant pre–September 11 conception that countering terrorism involved either the use of military force or enforcement of the criminal laws, counterterrorism law now incorporates a diverse range of responses to terrorism, many of which are borrowed, sometimes in modified form, from existing international and domestic law. Based on a maturing international legal regime, this article concludes that over time and through State practice, along with legal, strategy and policy development in the international community, a set of counterterrorism law norms for cyber war could emerge.

In this article, I will first review the *ad bellum* justifications for conducting cyber war within the Charter and LOAC systems. The international law doctrines permitting countermeasures offer one set of options, and the possibility that cyber intrusions could constitute an unlawful intervention, "use of force" or "armed attack" will also be considered briefly. I conclude that the Charter and LOAC provide insufficiently clear legal guidance, and

that further accommodating the various forms of cyber war could compromise the normative integrity of the existing system for limiting the use of force and may unnecessarily further militarize the cyber domain.[20] Part III traces the sources and contents of counterterrorism law that could provide the normative bases for cyber war in some circumstances. In light of the analysis in Parts II and III, Part IV will speculate concerning how an international counterterrorism law might develop in the cyber domain. As has been the case with counterterrorism law generally, a cyber-oriented counterterrorism law will follow the eventual development and implementation of national and international policies and strategies to counter cyber threats.

II. FINDING *AD BELLUM* JUSTIFICATION FOR CYBER WAR

Assume that the fictional State of Evil launches a massive malware attack at the fictional State of Bliss. The botnets and sophisticated software unleashed by the malware cause power failures when generators are shut down by the malware. Train derailments and airplane crashes with hundreds of casualties soon follow as traffic control and communications systems that rely on the Internet are made to issue false signals to pilots and conductors. Dozens of motorists die when traffic lights and signals malfunction at the height of an urban rush hour. Evil acknowledges its responsibility for the cyber attacks, and it says that more are on the way. Clearly there is an international armed conflict (IAC) between Evil and Bliss and, pending Security Council action, Bliss is lawfully permitted by Article 51 of the Charter to use self-defense to respond to the "armed attack" by Evil. The Charter and LOAC norms provide sufficient *ad bellum* authority for Bliss to respond to these cyber attacks.

Assume instead that a terrorist group has launched a series of cyber attacks on the banking system of a G-8 State. The malware is sophisticated; large and small customers' accounts are targeted and account balances are reduced by hundreds of millions of dollars. For the time being the attacks cannot be attributed to the terrorist group, but terrorists are suspected in light of intelligence reports. No one has been injured or killed. There is no IAC, either because there is no known State adversary either because there has been no "attack" as contemplated by Article 49 of the Third Geneva

20. *See* Mary Ellen O'Connell, *Cyber Security without Cyber War*, 17 JOURNAL OF CONFLICT AND SECURITY LAW 187, 190–91, 199 (2012).

Convention. There is no non-international armed conflict (NIAC), because the conflict is not sufficiently intense, or because the likely culprit is not an organized armed group. It is far from clear that there has been a "use of force" as contemplated by Article 2(4) of the Charter, or an "armed attack" within the meaning of Article 51. Surely the G-8 State must respond to deflect and/or dismantle the sources of the malware, and delaying responses until attribution is certain will greatly exacerbate the crisis. Under these circumstances, what *ad bellum* principles should determine the victim State's response?

Although these two simplistic scenarios do not fairly represent the wide range of possible cyber intrusions that occur now on a daily basis, they do underscore that only the most destructive cyber attacks fall clearly within the existing Charter and LOAC framework for cyber war. Why is fitting cyber within the traditional framework for armed conflict so difficult? What international law principles offer the best options for extending their application to cyber attacks?

One of the most challenging aspects of regulating cyber war is timely attribution. As Joel Brenner reminds us, "the Internet is one big masquerade ball. You can hide behind aliases, you can hide behind proxy servers, and you can surreptitiously enslave other computers to do your dirty work."[21] Cyber attacks also often occur in stages over time. Infiltration of a system by computers operated by different people in different places may be followed by delivery of the payload and, perhaps at a later time, manifestation of the harmful effects. At what stage has the cyber attack occurred? Attribution difficulties also reduce the disincentives to cyber attack and further level the playing field for cyber war waged by terrorists. Although identifying a cyber intruder can be aided by a growing set of digital forensic tools, attribution is not always fast or certain, making judgments about who was responsible for the cyber intrusion that harmed the victim State probabilistic.[22] Even where the most sophisticated forensics can reliably determine the source of an attack, the secrecy of those methods may make it difficult to demonstrate attribution in a publicly convincing way. Because the Charter- and LOAC-based *ad bellum* justifications for respond-

21. BRENNER, *supra* note 3, at 32.

22. *See* NATIONAL RESEARCH COUNCIL, TOWARD A SAFER AND MORE SECURE CYBERSPACE (Seymour E. Goodman & Herbert S. Lin eds., 2007); NATIONAL RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES § 2.4.2 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) [hereinafter TECHNOLOGY, POLICY, LAW, AND ETHICS].

ing to a cyber attack are tied to attribution of the attack and thus identification of the enemy, the legal requirements for attribution may at least delay effective defenses or responses.

The traditional approach to assessing *ad bellum* authority to respond to aggression involves assessing the consequences of the attack. What international law determines the permissible responses to a cyber attack that causes considerable economic harm but no physical damage? Is the loss or destruction of property sufficient to trigger a kinetic response? The answer turns in part on whether the State wishes to use force in response. For non-forceful responses, customary international law has long allowed countermeasures—lawful actions undertaken by an injured State in response to another State's internationally unlawful conduct.[23] In the cyber context, intrusions that fall short of armed attacks as defined by the Charter are nonetheless in violation of the international law norm of non-intervention and thus permit the reciprocal form of violation by the victimized State. As codified by the International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts, countermeasures must be targeted at *the State* responsible for the prior wrongful act, and must be temporary and instrumentally directed to induce the responsible *State* to cease its violation.[24]

In the cyber arena, one important question is whether countermeasures include so-called active defenses, which attempt through an in-kind response to disable the source of an attack while it is under way.[25] Whatever active defense technique is pursued by the victim State thus has a reciprocal relationship with the original cyber intrusion, and like the original intrusion the active defense presumptively breaches State sovereignty and violates the international law norm of non-intervention. (Passive defenses, such as firewalls, attempt to repel an incoming cyber attack.) Active defenses may be pre-set to deploy automatically in the event of a cyber attack, or they may be managed manually.[26] Computer programs that relay destructive vi-

---

23. U.N. International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, ch. II, U.N. GAOR, 53d Sess. Supp. No. 10, at 80, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 26, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2) [hereinafter *Draft Articles on Responsibility of States for Internationally Wrongful Acts*].

24. *Id.*, art. 49 (emphasis added).

25. *See* Eric T. Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, 38 STANFORD JOURNAL OF INTERNATIONAL LAW 207, 230 (2002).

26. *Id.* at 231.

ruses to the original intruder's computer or packet-flood the computer have been publicly discussed.[27] Although descriptions of most active defenses are classified, the United States has publicly stated that it employs "active cyber defense" to "detect and stop malicious activity before it can affect [Department of Defense] networks and systems."[28]

In theory, countermeasures provide a potentially effective defensive counter to cyber attacks. In practice, a few problems significantly limit their effectiveness. First, the Draft Articles codify customary law requirements that before a State may use active defense countermeasures it must find that an internationally wrongful act caused the State harm, identify the State responsible and follow various procedural requirements,[29] delaying execution of the active defense. The delay may be exacerbated by the problems in determining attribution. Second, note that countermeasures customarily are available in State-on-State conflicts, not in response to intrusions by a non-State actor. A non-State actor's actions may be attributable to a State when the State knows of the non-State actors' actions and aids them in some way,[30] or possibly when the State merely knowingly lets its territory be used for unlawful acts.[31] In most instances, however, international law supplies no guidance on countermeasures that respond to intrusions by non-State actors. Third, the normative principle that justifies countermeasures is that the initial attacker must find the countermeasure sufficiently costly to incentivize lawful behavior. For non-State terrorist groups that act independent of any State, a fairly simple relocation of their servers or other equipment may evade or overcome the countermeasures and remove any incentives to stop the attacks. In sum, although the countermeasures doctrine is well suited to non-kinetic responses to cyber attacks by States, attribution delays may limit their availability, and the line between permitted countermeasures and a countermeasure that constitutes a forbidden "use of force" is not clear. Nor do countermeasures apply in

---

27. *Id.*

28. U.S. Department of Defense, Department of Defense Strategy for Operating in Cyberspace (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf; *see also* Jensen, *supra* note 25, at 230.

29. *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, *supra* note 23, arts. 49–52.

30. *Id.*, art. 16.

31. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22 (Apr. 9). *See also* Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, 201 MILITARY LAW REVIEW 1, 43 (2009).

responding to a terrorist group unaffiliated with any State, and such groups are less likely to be incentivized by the countermeasures to stop their attacks.

Even if each of these limitations is overcome, the prevailing view is that active defenses may only be employed when the intrusion suffered by a victim State involves a "use of force" as interpreted at international law.[32] Note the potential for tautology in this legal analysis—"force" in the form of active defense is allowed in response because the responder labels the incoming intrusion a "use of force." Taken together, the promise of countermeasures in responding to cyber attacks is significantly compromised by problems of attribution, timing, efficacy and logic. At the same time, if active defense countermeasures are not considered as a "use of force," the attribution problem loses its urgency. There is no clear international barrier to non–use of force countermeasures, and attribution may be determined when feasible since no force is being used. Finally, the International Group of Experts that prepared the *Tallinn Manual* acknowledged that while victim States may not continue countermeasures after the initial intrusion had ended, State practice "is not fully in accord. . . . States sometimes appear motivated by punitive considerations . . . after the other State's violation of international law has ended."[33] In other words, customary law on cyber countermeasures is in flux.

After providing in Article 2(4) that all member States "shall refrain . . . from the threat or use of force against the territorial integrity or political independence of any state,"[34]Article 51 creates an exception to the strict prohibition by stating that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations."[35] The "use of force" rubric from Article 2(4) establishes the standard for determining a violation of international law. Once a use of force occurs, permissible responses are determined by the law of State responsibility,[36] potential Security Council resolutions and the law of self-defense. The traditional and dominant view among member States is that the prohibition on the use of force and right

32. Jensen, *supra* note 25, at 231.

33. TALLINN MANUAL, *supra* note 13, rule 9, cmt. 3.

34. U.N. Charter art. 2, para. 4.

35. *Id.*, art. 51.

36. *See* Michael N. Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited*, 56 VILLANOVA LAW REVIEW 569, 573–80 (2011).

of self-defense apply to armed violence, such as military attacks,[37] and only to interventions that produce physical damage. As such, most cyber attacks will not violate Article 2(4).[38] Throughout the Cold War, some States argued that the Article 2(4) "use of force" prohibition should focus not so much on the instrument as the effects of an intrusion and thus forbids coercion, by whatever means, or violations of sovereign boundaries, however carried out.[39] The United States opposed these efforts to broaden the interpretation of "use of force" by developing States, and by the end of the Cold War Charter interpretation had settled on the traditional and narrower focus on armed violence.[40]

Article 2(4) is textually capable of evolving to include cyber intrusions, depending on the severity of their impact. Cyber attacks can cause harm equivalent to kinetic attacks. The imprecision of the text and the growing cyber threat suggests that State practice may now or will in the future recognize cyber intrusions as "uses of force," at least when cyber attacks deliver consequences that resemble those of conventional armed attacks.[41] Public statements by the United States in recent years suggest that our government is moving toward this sort of effects-based interpretation of the Charter's use-of-force norm in shaping its cyber defense policies, a position at odds with our government's history of resisting flexible standards for interpreting Article 2(4).[42] As historically interpreted, however, the Charter

37. TECHNOLOGY, POLICY, LAW, AND ETHICS, *supra* note 22, at 253.

38. *See* Jason Barkham, *Information Warfare and International Law on the "Use of Force,"* 34 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 56 (2001).

39. Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4),* 36 YALE JOURNAL OF INTERNATIONAL LAW 421, 428 n.32, 429–30 nn.37–38 (2011).

40. *Id.* at 431.

41. TECHNOLOGY, POLICY, LAW, AND ETHICS, *supra* note 22, at 33-34; Waxman, *supra* note 39, at 432 n.48 (citing Abraham D. Sofaer et al., *Cyber Security and International Agreements, in* COMMITTEE ON DETERRING CYBERATTACKS, NATIONAL RESEARCH COUNCIL, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 179, 185 (2010)). *See also* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 914–15 (1999) (proposing that cyber attacks could constitute use of force if they meet several practical measures of harm). *See also* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIFORNIA LAW REVIEW 817, 848 (2012); THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 14 (2011) [hereinafter INTERNATIONAL STRATEGY FOR CYBERSPACE]; *see also* TALLINN MANUAL, *supra* note 13, rule 11.

42. Waxman, *supra* note 39, at 436–37. *See* Ellen Nakashima, *U.S. official says cyberattacks can trigger self-defense rule*, WASHINGTON POST (Sept. 18, 2012), http://articles.washing

purposefully imposes an additional barrier to a forceful response to a use of force. The response to such a use of force cannot itself rise to the level of use of force unless authorized by the Security Council or unless it is a lawful action in self-defense.[43] In other words, unilateral responses to a use of force are permitted only if the intrusion constitutes an armed attack recognized by Article 51.

To the extent that cyber intrusions do not meet the criteria for "use of force," Russell Buchan argues that cyber attacks that do not cause physical damage violate international law on the basis of the principle of non-intervention as embodied in customary law.[44] Buchan maintains that non-intervention proscribes cyber attacks that are not destructive so long as the attack is intended to coerce a victim State into a change in policy "in relation to a matter that the victim State is freely entitled to determine itself."[45] Although the non-intervention norm has the potential to serve as a legal barrier to disruptive cyber intrusions, there is no indication that any State has relied on Buchan's argument, or that any court has credited it in a cyber context.

Some scholars have argued that cyber attacks that are especially destructive but have not traditionally been considered armed attacks under Article 51 might nonetheless give rise to the Article 51 right of self-defense.[46] But no international tribunal has so held. In a case involving conventional armed violence, but on a small scale, the United States argued unsuccessfully before the International Court of Justice (ICJ) that its naval attacks on Iranian oil platforms were justified by the right of self-defense following low-level Iranian attacks on U.S. vessels in the Persian Gulf.[47] Although the separate opinion of Judge Simma in the *Oil Platforms* case ar-

---

tonpost.com/2012-09-18/world/35497194_1_international-law-legal-adviser-cyberspace (noting that State Department Legal Adviser Harold Koh stated that any use of force triggers the right of self-defense, and cyber attacks that result in injury, death, or significant destruction would be seen as a violation of international law).

43. *See* Vida M. Antolin-Jenkins, *Defining the Parameters of Cyberwar Operations: Looking for Law in All the Wrong Places?*, 51 NAVAL LAW REVIEW 132, 172–74 (2005) (concluding that the "use of force" and "armed attack" formulations do not apply to all but a few of the most extreme cyber incidents).

44. Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 JOURNAL OF CONFLICT AND SECURITY LAW 211, 214 (2012).

45. *Id.* at 224.

46. Jensen, *supra* note 25, at 223–39; Schmitt, *supra* note 41, at 930–34; *see also* TALLINN MANUAL, *supra* note 13, rule 13, cmt. 9.

47. Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶¶ 46–47 (Nov. 6).

gued that self-defense should permit more forceful countermeasures where the "armed attack" threshold has not been met,[48] this more flexible approach has not been accepted by the ICJ or any court, and only State practice is likely to change the prevailing traditional interpretation.

In any case, the "use of force" framework has little value in developing responses to terrorists. By the terms of the Charter, non-State actors cannot violate Article 2(4), and responses to uses of force are limited to actions carried out by or otherwise the responsibility of States.[49] Guidance on the degree of State control that must exist to establish State liability for a non-State group's actions was supplied by the ICJ in the *Nicaragua* case, where the Court limited U.S. responsibility for actions of the Nicaraguan Contras to actions where the United States exercised "effective control of the military or paramilitary operations [of the Contras] in the course of which the alleged violations were committed."[50] Only if the State admits its collaboration with terrorists[51] or is otherwise found responsible for the terrorists' actions may the victim State use force against the terrorists and sponsoring State.

In recent years, the law of self-defense has been at the center of international law attention. Yet for better or worse, the legal doctrine remains unsettled. The text of Article 51—"armed attack"—is not as amenable as "use of force" to a flexible interpretation (the phrase "armed attack" is relatively precise). Nor did the Charter drafters consider the possibility that very harmful consequences could follow from a non-kinetic, cyber attack. Nonetheless, outside the cyber realm State practice has evolved toward accepting that attacks by terrorists may constitute an armed attack that triggers Article 51 self-defense.[52] The text of Article 51 does not limit armed

48. *Id.*, ¶ 12 (opinion of Simma, J.).

49. *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, *supra* note 23, art. 8.

50. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶¶ 115, 109 (June 27). A somewhat different approach was taken by the International Criminal Tribunal for the former Yugoslavia in *Tadić*, where the Court focused on whether the Federal Republic of Yugoslavia exercised "overall control" of the Bosnian Serb armed groups. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶ 145 (Int'l Crim. Trib. for the former Yugoslavia July 15, 1999).

51. *See Draft Articles on Responsibility of States for Internationally Wrongful Acts*, *supra* note 23, art. 11.

52. Steven R. Ratner, *Self-Defense Against Terrorists: The Meaning of Armed Attack, in* LEIDEN POLICY RECOMMENDATIONS ON COUNTER-TERRORISM AND INTERNATIONAL LAW (Nico Schrijver & Larissa van den Herik eds., forthcoming 2012); Michael N. Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum*: A Normative Framework*, 56 NA-

attacks to actions carried out by States, although the State-centric model of the Charter strongly suggests that the drafters contemplated only those armed attacks by non-State actors that could be attributed to a State as Article 51 armed attacks.

The dramatic development that made it clear that armed attacks may occur by non-State terrorists regardless of the role of a State was 9/11. Within days of the attacks, the Security Council unanimously passed Resolutions 1368 and 1373 and recognized "the inherent right of individual or collective self-defense in accordance with the Charter" in responding to the attacks.[53] NATO adopted a similarly worded resolution.[54] Unlike prior instances where non-State attackers were closely linked to State support, the Taliban merely provided sanctuary to al Qaeda and did not exercise control and were not substantially involved in al Qaeda operations.[55]

State practice in the international community supported extending self-defense as the *ad bellum* justification for countering al Qaeda on a number of occasions since 2001.[56] While the ICJ has not ratified the evolving State practice, and even seemed to repudiate it in at least three decisions—twice since 9/11[57]—the trend is to accept the extension of armed attack self-

---

VAL LAW REVIEW 1, 7–13 (2008). Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts, in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS, *supra* note 41, 151, 163–64; Sean Watts, *Low-Intensity Computer Network Attack and Self-Defense,* INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 59, 75–76 (Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies); Office of General Counsel, U.S. Department of Defense, An Assessment of International Legal Issues in Information Operations 16 (May 1999), *available at* http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf [hereinafter An Assessment of International Legal Issues]; *see also* TALLINN MANUAL, *supra* note 13, rule 13, cmt. 16 (majority of the Group of Experts agree that a cyber attack by terrorists may constitute an armed attack).

53. S.C. Res. 1368, U.N. Doc. S/RES/1368 (Sept. 12, 2001); S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001).

54. Press Release, North Atlantic Treaty Organization, Statement by the North Atlantic Council (Sept. 12, 2001), *available at* http://www.nato.int/docu/pr/2001/p01-124e.htm.

55. *See* Derek Jinks, *State Responsibility for the Acts of Private Armed Groups*, 4 CHICAGO JOURNAL OF INTERNATIONAL LAW 83, 89 (2003).

56. Ratner, *supra* note 52, nn.5–6.

57. In the *Nicaragua* case, the ICJ never considered whether paramilitary activity by the contras or the FMLN was an armed attack, and focused only on whether their activities could be imputed to the States involved. In *Armed Activities on the Territory of the Congo*, the Court stated that attacks by armed groups could not trigger Article 51, because they

defense authorities when non-State groups are responsible, provided the armed attack predicate is met and the group is organized and not a set of isolated individuals.[58] Unsurprisingly, the U.S. Department of Defense supports the same position.[59] Thus, despite the apparent gulf between the text of the Charter as interpreted by the ICJ and State practice, whether an "armed attack" is kinetic or cyber-based, armed force may be used in response to an imminent attack if it reasonably appears that a failure to act promptly will deprive the victim State of the opportunity to defend itself.[60]

The legal bases for self-defense have similarly been extended to anticipatory self-defense in the cyber context. As evolved from Secretary of State Daniel Webster's famous formulation in response to the *Caroline* incident that self-defense applies in advance of an actual attack when the "necessity of that self-defence is instant, overwhelming, and leaving . . . no moment for deliberation,"[61] contemporary anticipatory self-defense permits the use of force in anticipation of attacks that are imminent, even if the exact time and place of attack are not known.[62] Imminence in contemporary contexts is measured by reference to a point in time where the State must act defensively before it becomes too late.[63] In addition to imminence or immediacy, the use of force in self-defense must be necessary—law enforcement or

---

were "non-attributable to the DRC," though at another point the Court stated that it would not address whether self-defense applies against "large-scale attacks by irregular forces." Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶¶ 146–47 (Dec. 19). In the *Wall* opinion, the Court maintained that self-defense is available in State-on-State conflicts, and found self-defense inapplicable partly because Israel did not allege that the harmful acts were imputable to a foreign State. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, § 139 (July 9).

58. *See, e.g.,* U.N. Secretary-General, *Report of the Secretary-General's Panel of Inquiry on the 31 May 2010 Flotilla Incident*, Annex 1, § 41, at 93 (Sept. 2011); Ratner, *supra* note 52, at 8–9.

59. Ratner, *supra* note 52, n.32

60. Schmitt, *supra* note 36, at 593.

61. Letter from Daniel Webster, U.S. Secretary of State, to Lord Ashburton, British Special Minister (Aug. 6, 1842), *reprinted in* 2 JOHN MOORE DIGEST OF INTERNATIONAL LAW 411–12 (1906).

62. *See, e.g.*, THE WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 22 (2010).

63. Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum, *supra* note 52, at 16–19; *see also* TALLINN MANUAL, *supra* note 13, rule 15 (describing variations on an imminence requirement).

other non–use of force means will not suffice—and the attacking group must be shown to have the intent and means to carry out the attack.[64]

In contemporary State practice, nearly every use of force around the world is justified as an exercise of self-defense.[65] As Sean Watts has observed, "in the post-Charter world . . . States have resurrected pre-Charter notions that self-defense includes all means necessary for self-preservation against all threats."[66] In this environment of expansive interpretations of self-defense relatively unbounded by positive law, the legal parameters of self-defense law as just summarized may be applied to the cyber domain and adapted to cyber attacks, subject to meeting the Article 51 threshold of armed attack. Applied to non-State actors, if a cyber attack by a non-State actor constitutes an armed attack as contemplated by the Charter, self-defense allows the victim State to conduct forceful operations in the State where the terrorist perpetrators are located *if* the latter State is unable or unwilling to police its territory. In the sphere of anticipatory self-defense, the fact that cyber attacks will come unattributed and without warning provides strong analogs to the challenges of counterterrorism law. At the same time, even though reliance on self-defense arguments is and will remain tempting in the cyber arena, the value of the Charter system in making law for new cyber-response applications is limited by the "use of force" and "armed attack" qualifications.

What do the Charter, LOAC and emerging State practice say about cyber attacks that do not meet the armed attack threshold? One potentially important rule distilled from the Charter and State practice is that a number of small cyber attacks that do not individually qualify as armed attacks might do so when aggregated, provided there is convincing evidence that the same intruder is responsible for all of the attacks.[67] The so-called pin-prick theory could have emerging importance in supporting cyber self-defense, especially if technical advances aid in attribution. Otherwise, distilling the conclusions in this section, the international law of self-defense may only justify responses to cyber attacks that are sufficiently destructive to meet the armed attack threshold, a small subset of cyber intrusions. Still, in limited situations, if a cyber intrusion is believed to be caused by a non-State terrorist organization (through actual attribution or meeting an immi-

64. Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum, *supra* note 52, at 18–19.

65. Watts, *supra* note 52, at 87 n.142.

66. *Id.* at 76.

67. TALLINN MANUAL, *supra* note 13, rule 13, cmt. 8.

nence requirement in anticipatory self-defense), and the intrusion is sufficiently disruptive as to cause significant harm to important functions in society but does not meet the traditional armed attack criteria, it remains possible that Article 51 self-defense authority may be extended to permit forceful countermeasures or other forceful responses to a cyber attack, based on State practice. Whether the development of cyber law so removed from the text of the Charter represents the optimal path forward for the law of cyber war will be considered in the final section of this article. On the one hand, the Charter's self-defense doctrine as traditionally understood may not leave States adequate authority to respond to the full range of cyber threats they face. On the other hand, the development of customary law through State practice is the ultimate flexible vehicle for making new law to confront emerging problems. Even Charter law interpreted at degrees of separation from the Charter is preferable to a legal vacuum.[68] We will see that counterterrorism law may contribute to the development of an international legal paradigm for cyber defense without producing additional strain on traditional *ad bellum* norms.

III. THE POTENTIAL FOR APPLICATION OF COUNTERTERRORISM LAW

Counterterrorism law is immature, in flux and heavily contested. This section will show that, despite resistance from many quarters and a two-steps-forward-one-step-back development in the United States, counterterrorism law deserves recognition as a discrete and integral part of international law. As the international community gradually embraced the idea that violent terrorism by non-State actors justifies the use of force pursuant to the *jus ad bellum*, several treaties and agreements, Security Council resolutions, and State practice are beginning to recognize counterterrorism law as a sort of hybrid blend of several components of international law. The cyber domain is not yet part of the new corpus, but its time may have arrived.

As Adam Roberts noted more than ten years ago, counterterrorism operations are not entirely like or unlike armed conflicts or other wars.[69] The fact that counterterrorism involves the use of military force along with pursuit of law enforcement and other non–use of force methods involves awkward confluences with international law generally and with *ad bellum*

68. *See* Watts, *supra* note 52, at 66.

69. Adam Roberts, *The Laws of War in the War on Terror*, *in* INTERNATIONAL LAW AND THE WAR ON TERROR 175, 227–28 (Fred L. Borch & Paul S. Wilson eds., 2003) (Vol. 79, U.S. Naval War College International Law Studies).

and *in bello* principles in particular. By and large, the awkwardness has been explained away by international law scholars in the past in their assertions that there simply is no international law concerning terrorism.[70] Undeniably, however, there is now an evolving international counterterrorism law. Through thirteen international treaties, several Security Council resolutions, State practice and emerging policies counterterrorism is developing as an international law paradigm in ways similar to human rights law development in earlier years.[71] The counterterrorism methods are not new, for the most part, and the counterterrorism paradigm does not so much reject the LOAC/armed conflict/war models as offer a complement to them.

That the field of international counterterrorism law is gaining recognition among practitioners and scholars is reflected by the publication of two comprehensive treatises covering counterterrorism law in recent years, each with a stable of distinguished jurists, lawyers and scholars as contributors, and both intent on surveying the state of law in a growing and complex field.[72] Selections from their combined tables of contents are illustrative: counterterrorism and the rule of law framework, multidisciplinary perspectives, UN counterterrorism instruments, judicial and non-judicial responses to terrorism, criminal laws and jurisdiction, investigations and prosecutions, pretrial and trial issues, combating terrorism financing, alternative remittance systems, human rights in countering terrorism and international cooperation.[73] As explained by Katja Samuel in the 2012 volume of *Counter-Terrorism: International Law and Practice*, the "backbone of the existing international [counterterrorism] rule of law framework" consists of human rights law, humanitarian law, criminal law and refugee/immigration law, along with the Charter and general international law principles.[74]

Just as it is noteworthy that international counterterrorism law has emerged as a discrete field, the omission of any treatment of international cyber law in the treatises is striking. In the cyber realm, instead of treating

---

70. *See, e.g.*, Higgins, *supra* note 5; BROWNLIE, *supra* note 5.

71. *See* Daniel Moeckli, *The Emergence of Terrorism as a Distinct Category of International Law*, 44 TEXAS INTERNATIONAL LAW JOURNAL 157, 167–68 (2008). *See also* Cohen, *supra* note 4.

72. AVINDER SAMBEI ET AL., COUNTER-TERRORISM LAW AND PRACTICE (2009); COUNTER-TERRORISM: INTERNATIONAL LAW AND PRACTICE, *supra* note 12.

73. SAMBEI ET AL., *supra* note 72; COUNTER-TERRORISM: INTERNATIONAL LAW AND PRACTICE, *supra* note 12.

74. Katja L.H. Samuel, *The Rule of Law Framework and its Lacunae: Normative, Interpretive, and/or Policy Created?*, *in* COUNTER-TERRORISM: INTERNATIONAL LAW AND PRACTICE, *supra* note 12, at 14.

cyber attacks by terrorists in the either/or dichotomy as crimes or equivalent to kinetic attacks, counterterrorism law may prescribe a range of responses, including intelligence collection and threat identification, border controls, asylum and refugee status rules and procedures, controls on providing financial support to terrorists and kinetic options, the contents of which may vary from traditional LOAC use of force, depending on the harm caused by the attacks. Particularly over the decade after 9/11, counterterrorism matured as a legal regime composed of primary rules, including Security Council resolutions requiring that States take steps to counter terrorism and various treaties, and secondary rules that monitor enforcement of the counterterrorism tools and add norms to counterterrorism in subsidiary areas, such as international criminal law and armed conflict.[75] Unsurprisingly, the development of an international law of counterterrorism reflects parallel developments at the national level in many States.[76]

Counterterrorism law is similarly evolving as domestic law in the United States. Before the 9/11 attacks, the U.S. Army defined counterterrorism as "offensive military operations designed to prevent, deter and respond to terrorism."[77] The Defense Department recognized after 9/11 that "some significant policy and strategy adjustments were required"[78] to counterterrorism doctrine owing to the evolution of the terrorist threat and to conform U.S. military doctrine to international law (the pre-9/11 definition may have permitted actions in violation of Article 2(4) of the Charter). The National Security Strategy of the United States also gradually showed a maturing understanding of the role of counterterrorism. The 2002 Strategy became immediately controversial because of its articulation of an apparent doctrine of preemption.[79] By 2006, the preemption language was moved from the section on terrorism to a section focusing on weapons of mass destruction, and the Strategy recognized that the counterterrorism paradigm involves more than criminal law enforcement and reorientation of the

---

75. Moeckli, *supra* note 71, at 167–68. *See also* Gregory E. Maggs, *Assessing the Legality of Counterterrorism Measures without Characterizing Them as Law Enforcement or Military Action*, 80 TEMPLE LAW REVIEW 661 (2007).

76. *See generally* GLOBAL ANTI-TERRORISM LAW AND POLICY (Victor V. Ramraj et al. eds., 2d ed. 2012).

77. Chairman, Joint Chiefs of Staff, Joint Publication 3-26, Counterterrorism v (2009) [hereinafter Joint Publication 3-26].

78. *Id.*

79. THE WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 15 (2002).

norms for war.[80] Concerning the use of force in counterterrorism, the measure of imminence in self-defense had evolved in domestic law as it had in international law due to the anonymity and surprise factors in terrorist attacks and was measured as much by the availability of an opportunity to respond as by the immediacy in time of the anticipated attack.[81] Likewise, territorial sovereignty weakened as a barrier to action in self-defense.[82] By 2009, the Department of Defense had broadened considerably its definition of counterterrorism: "actions taken directly against terrorist networks and indirectly to influence and render global and regional environments inhospitable to terrorist networks."[83] So understood, counterterrorism "is an activity of irregular warfare" and its "efforts should include all instruments of national power to undermine an adversary's power and will, and its credibility and legitimacy to influence the relevant population."[84]

As a baseline proposition, in the twenty-first century there can be little doubt that violent terrorism justifies the use of force in countering terrorist attacks pursuant to the *jus ad bellum*. Any shortcomings in the normative foundation for counterterrorism law were effectively erased after the 9/11 attacks and passage of Security Council Resolutions 1373 and 1377. Even in the years before 9/11, the Security Council recognized that terrorism could constitute a breach of peace and security.[85] Although the Council has not authorized the use of force in response to terrorism, it could do so.[86] The Counterterrorism Committee of the United Nations Security Council was established in 2001 by Resolution 1373, which determined "to combat by all means threats to international peace and security caused by terrorist

80. THE WHITE HOUSE, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 23 (2006).

81. *See* Watts, *supra* note 52.

82. Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum, *supra* note 52, at 27–30.

83. Joint Publication 3-26, *supra* note 77, at vi.

84. *Id.* at viii.

85. *See, e.g.*, S.C. Res. 1189, U.N. Doc. S/RES/1189 (Aug. 13, 1998) (sanctions imposed following terrorist bombings in Kenya and Tanzania).

86. Schmitt, *Responding to Transnational Terrorism under the* Jus Ad Bellum, *supra* note 52, at 2–5. *See also* Watts, *supra* note 52, at 64–65; North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 34 U.N.T.S. 243; William Howard Taft IV, *The Bush (43rd) Administration, in* SHAPING FOREIGN POLICY IN TIMES OF CRISIS: THE ROLE OF INTERNATIONAL LAW AND THE STATE DEPARTMENT LEGAL ADVISOR 127, 128–29 (Michael P. Scharf & Paul R. Williams eds., 2010) ("[We] had no difficulty in establishing that we had a right to use force in self-defense against Al-Qaeda and any government supporting it . . . .").

acts"[87] and commended all States to take necessary steps to prevent terrorism and ensure that terrorist acts are established as criminal offenses in domestic laws. Resolution 1373 also obliged member States to prevent the financing of terrorism; criminalize the collection of funds for terrorist purposes; freeze the financial assets of anyone who participates in, or facilitates, terrorism; take any steps necessary to prevent terrorist acts, including passing early-warning information to other States; suppress recruitment of members of terrorist groups; eliminate the supply of weapons to terrorists; deny safe haven to those involved in terrorism; and ensure that serious criminal penalties are established for all terrorist acts.[88]

In 2006 the General Assembly adopted the Global Counter-Terrorism Strategy and embraced what it called a common framework to fight terrorism.[89] The General Assembly recognized that counterterrorism law incorporates a multifaceted set of tools that relies on the legal principles in LOAC, human rights law, refugee and asylum law, and criminal law, along with the Charter, to constitute its framework.[90] Despite the aspirations of the General Assembly, however, more recently the World Justice Project agreed that "there is as yet no fully coherent international legal regime governing terrorism and responses to terrorism."[91] Although counterterrorism law has developed in recent years, the World Justice Project is correct, and the high visibility of cyber threats may provide incentives to further develop counterterrorism law as a set of international law norms.

In practice, counterterrorism law has evolved as something of a hybrid species of law, blending parts of conventional domestic criminal laws and procedures with modified LOAC principles, components of human rights

87. S.C. Res. 1373, *supra* note 53.

88. *Id.* Resolution 1373 has been described as "one of the most comprehensive and far-reaching resolutions adopted in the history of the Security Council." Curtis A. Ward, *Building a Capacity to Combat International Terrorism: The Role of the United Nations Security Council*, 8 JOURNAL OF CONFLICT AND SECURITY LAW 289, 298 (2003).

89. G.A. Res. 60/288, U.N. Doc. A/RES/60/288 (Sept. 8, 2006) (reviewed by the U.N. General Assembly biennially in G.A. Res. 62/272, U.N. Doc. A/RES/62/272 (Sept.5, 2008); G.A. Res. 64/297, U.N. Doc. A/RES/64/297 (Sept. 8, 2010); G.A. Res. 66/282, U.N. Doc. A/RES/66/282 (June 29, 2012)).

90. G.A. Res. 60/288, Action Plan: Preamble, Pillar IV, *supra* note 89, ¶¶ 2–5.

91. KATJA SAMUEL, NIGEL D. WHITE, ANA MARIA SALINAS DE FRÍAS, WORLD JUSTICE PROJECT COUNTER-TERRORISM EXPERT NETWORK, REPORT OF KEY FINDINGS AND RECOMMENDATIONS ON THE RULE OF LAW AND COUNTER-TERRORISM 12 (2012). The World Justice Project would locate the undefined remaining corpus of counterterrorism law in criminal laws. *Id.* at 56.

law, and refugee and asylum law.[92] By any standard, the evolution of counterterrorism law has not been easy or devoid of controversy. For example, over the last decade, opponents of U.S. domestic counterterrorism policies frequently argued that some of the measures taken, such as law of war detention and rendition, violated domestic law guarantees designed to protect criminal suspects. Our government responded that, in the ongoing counterterrorism campaign, the LOAC rules applied in a "new kind of war" and were being followed.[93] More recently, the counterterrorism targeted-killing policy initiated by the George W. Bush administration and expanded by President Obama remains controversial, in part because it reflects neither traditional law enforcement nor LOAC doctrines, but contains elements of both, and some components that are unique to counterterrorism.[94] More particularly, in the implementation of the targeting policy, positive identification of the target is required, although the lawful target is not a combatant in LOAC terms. The LOAC principle of distinction applies, and the military commander in charge of the targeting operation is instructed to capture the terrorist suspect if that option is available, so long as the suspect poses no imminent danger to the U.S. force or those around him. The targeting may occur wherever the target is found, but will not be carried out where law enforcement personnel are capable of interdicting the target using lawful means.[95]

In a similar vein, the 2006 Israeli Supreme Court *Targeted Killings* decision recognizes counterterrorism law as a distinct legal paradigm, in a sort of back-handed way. In the Court's opinion, instead of treating potential targets as either civilians or combatants according to the LOAC framework, the Court said that they are citizens sometimes taking part in hostilities, so that they may be targeted at only certain times.[96] Although the Israeli decision continues to focus on whether the government program involves law enforcement or military action and thus fails to acknowledge the

92. *See* Moeckli*, supra* note 71, at 168.

93. *See id.* at 164–65; Memorandum from Alberto R. Gonzales, Counsel to the President, Office of Counsel to the President, to George W. Bush, President of the United States, Decision re Application of the Geneva Convention on Prisoners of War to the Conflict with Al Qaeda and the Taliban (Jan. 25, 2002), *available at* http://www.torturingdemocracy.org/documents/20020125.pdf.

94. *See* STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 376–410 (5th ed. 2011).

95. *Id.*

96. *See* Public Committee against Torture in Israel v. Government of Israel, HCJ 769/02, Judgment (Dec. 13, 2006), 46 INTERNATIONAL LEGAL MATERIALS 373 (2007), *available at* http://elyon1.court.gov.il/files_eng/02/690/007/a34/02007690.a34.pdf.

range of counterterrorism components, the Court did recognize that the dichotomy between military action and criminal law enforcement is insufficient and that counterterrorism does not fit in either of those paradigms neatly or completely.

The 2010 U.S. Department of Defense Quadrennial Defense Review acknowledged that counterterrorism requires a "portfolio of capabilities,"[97] including gathering intelligence about terrorist suspects through a variety of human and technical means, apprehending persons believed to be connected with terrorist attacks, freezing terrorist financial assets and imposing other financial sanctions, interdicting illicit trafficking in weapons and drugs that furthers terrorism, patrolling borders and transit hubs, establishing regulatory best-practice standards for private-sector infrastructure, mounting counter-radicalization programs, and pursuing community resilience initiatives. The May 2011 White House International Strategy for Cyberspace declared that "the United States will defend its networks . . . from terrorists . . . and dissuade and deter those who threaten peace and stability through actions in cyberspace . . . with overlapping policies that combine national and international network resilience with vigilance and a range of credible defense options."[98]

The strategy treats cyber as an operational domain, like air, sea and land.[99] Applied to the cyber domain, counterterrorism law could support a variety of responses, including active defenses, other economic, intelligence and law enforcement operations, and kinetic responses, depending on the degree of harm caused by the attacks. Counterterrorism techniques in the cyber realm may include intelligence devices that locate and identify cyber terrorists and their equipment, information campaigns to counter terrorist propaganda, and techniques that seek to learn about and infiltrate illicit cyber activities and/or destroy the proliferation of cyber weapons and techniques. The final section takes a preliminary look at how counterterrorism law could contribute to the normative architecture for cyber war.

97. U.S. DEPARTMENT OF DEFENSE, QUADRENNIAL DEFENSE REVIEW REPORT 20 (2010).

98. INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 41, at 12.

99. *Id.* at 6.

IV. *AD BELLUM* JUSTIFICATIONS FOR CYBER WAR—THE ROLE OF COUNTERTERRORISM LAW

For a long time there has been a tendency among some U.S. government officials and legal scholars to denigrate the status of international law generally and/or to claim that international law, whatever its role elsewhere, should not inform law judgments made by U.S. courts or our elected leaders. In the fields of national security and counterterrorism, however, spurred by the often eloquent and remarkably able efforts of State Department legal advisers and others over several recent administrations, we have also learned that international law has, in fact, played a major role in shaping national security and counterterrorism policies and operations, and that international law has been respected by senior U.S. officials of both parties.

Yet the "Global War on Terror" era in the years immediately after 9/11 and the invasion of Iraq without Security Council authorization in 2003 led many critics to observe that the United States was going its own way legally, at the expense of international law and the harmony of international relations among traditional allies. During the second term of President George W. Bush and throughout the Obama administration considerable effort has been made to articulate the international law bases for U.S. actions in pursuit of national security and counterterrorism objectives abroad, and the relative openness of administration lawyers about the law, including international law, has helped restore some confidence that international law matters in our government's decision-making calculus.

At the same time that U.S. government lawyers and decision makers have been working to create a set of coherent and harmonious domestic and international legal prescriptions for high-profile security and counterterrorism operations abroad, such as detention and targeting,[100] the incredibly fast pace of evolving cyber war has quickly outstripped our capacity for building and implementing an integrated domestic and international law architecture. In other words, at a time when counterterrorism law is contested and in flux and cyber threats are emerging as a central national security concern, international lawmakers may benefit by dealing with the two spheres at the same time. We are playing from behind, doing our best working with LOAC, the Charter and operational law decisions. Fortunate-

100. *See* Robert M. Chesney, *Beyond the Battlefield, Beyond Al Qaeda: The Destabilizing Legal Architecture of Counterterrorism*, xxx MICHIGAN LAW REVIEW (forthcoming 2013), draft *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2138623.

ly, ongoing research supported by the Department of Defense's Minerva program at the Massachusetts Institute of Technology and Harvard on the development of cyber norms[101] and events such as the Naval War College/U.S. Cyber Command Conference on Cyber War and International Law that spurred this article can help to shore up the legal architecture for cyber war.

In some cyber war settings, the still-evolving counterterrorism law could provide the international law corpus with new norms that account for the unique qualities and challenges of cyber. Reconsider defensive cyber operations and the attribution problem. Given the practical difficulties in obtaining prompt attribution of incoming cyber attacks and further assuming that the speed of operations requires active defenses in the event of a destructive or highly disruptive cyber attack, the imminence requirement in self-defense may be modified to reflect the characteristics of cyber. Borrowing from the lessons of countering kinetic terrorism, imminence or immediacy may no longer be measured only as a function of time, but includes an additional consideration—when is the last opportunity to take action to thwart or blunt the attacks? Cyber attacks, like kinetic terrorism, arrive with no warning. Surprise is the attacker's asymmetric advantage in targeting the victim State. Depending on the gravity of the attack, the costs of waiting for the attack before responding may be unconscionably high. Nor is it reasonable to build into the calculus of cyber defense any expectation that cyber attackers will abide by legal requirements such as avoiding harm to civilians and their property.[102] As such, counterterrorism law could complement the evolving interpretation of Article 51 self-defense by developing a nuanced and context-specific normative base for responding to destructive or especially disruptive cyber attacks. The Charter framework could remain more closely aligned with its overarching military force orientation, and the new counterterrorism law could develop in ways that will be briefly explored in this section.

In 2004, the Berlin Declaration on Upholding Human Rights and the Rule of Law in Combating Terrorism of the International Commission of Jurists stated that "in adopting measures aimed at suppressing acts of terrorism, states must adhere strictly to the rule of law, including core principles of . . . international law. . . and, where applicable, humanitarian law.

101. *See* EXPLORATIONS IN CYBER INTERNATIONAL RELATIONS, http://ecir.mit.edu/research/publications (last visited Nov. 30, 2012).

102. *See* Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum, *supra* note 52, at 16–20.

These principles . . . define the boundaries of permissible and legitimate state action against terrorism."[103]

Despite the best efforts of some of the keenest legal minds and most lucid juridical and scholarly formulations, international law generally and LOAC in particular do not supply a clear, complete and coherent *ad bellum* framework for cyber war. The "use of force" and "armed attack" thresholds were written to limit kinetic actions. Using persuasive arguments that the measure of invoking these gateway articles of the Charter should be practical, based on the effects of a cross-border intrusion and not on the nature of the instruments that cause the effects, Michael Schmitt and others have shown how cyber attacks may cause harm that should count as uses of force and, less plausibly, armed attacks. Their view is that once the gateway determinations are made to reach the cyber domain, LOAC supplies at least a serviceable road map for limiting cyber war.

In activating U.S. Cyber Command in 2010, the Department of Defense confronted congressional skepticism and challenges from across the political spectrum that focused on the Command's capabilities for interfering with the privacy rights of citizens, the policies and authorities that would define its mission, and its relationship to the nation's largely privately held critical infrastructure.[104] While Congress and other interested constituencies have continued to wrestle with the policy, scope of authorities, and privacy questions, from the beginning Cyber Command and the Department of Defense generally have indicated that existing Charter and LOAC-based law adequately support the authorities of the United States to defend the United States from cyber attack.[105] As this article has shown, however, there is no consensus that the Charter schema supplies a coherent or adequate set of norms for regulating cyber warfare. Particularly for cyber attacks that are especially disruptive but not destructive—intrusions that may be increasingly pervasive, operating beneath the radar of existing defensive mechanisms, and capable of fairly easily and cheaply being perpetrated by virtually any State or non-State actor—the Charter provides only the sketchiest of normative blueprints. The recurring theme of the LOAC

---

103. INTERNATIONAL COMMISSION OF JURISTS (ICJ), THE BERLIN DECLARATION: THE ICJ DECLARATION ON UPHOLDING HUMAN RIGHTS AND THE RULE OF LAW IN COMBATING TERRORISM, at pmbl. (Aug. 28, 2004).

104. Ellen Nakashima, *Cyber Command Chief Says Military Computer Networks Are Vulnerable*, WASHINGTON POST, (June 4, 2010), http://www.washingtonpost.com/wp-dyn/content/article/2010/06/03/AR2010060302355.html.

105. Watts, *supra* note 52, at 79 n.4. *See also id.* at 87 nn.139, 143.

bifurcation of international relations into states of war and peace is prominently displayed in the cyber arena. If the armed attack threshold is met, forceful responses may be employed. Otherwise only "peaceful" defenses are lawful. The asymmetric opportunities for non-State adversaries abound, and under the Charter norms victim States may have to choose between defending themselves unlawfully and absorbing continuing cyber attacks.[106]

Starting with the text of the Charter, this article has shown that arguments to apply the "use of force" and "armed attack" Charter categories to cyber may be based on a tautology—if the incoming cyber intrusion is construed as an armed attack, the victim State may respond in kind; if not so construed, the same or a similar response may not be considered an armed attack.[107] The fact that it may be possible simply to characterize a new form of intrusion—cyber attack—as a use of force or armed attack is not wholly satisfying analytically and, over time, such tautological reasoning may diminish the normative values embedded in these critical cornerstones of the Charter. In a similar vein, State practice in shaping responses to cyber intrusions has been characterized as applying a "know it when you see it"[108] approach to deciding when the intrusion constitutes a "use of force" or "armed attack" that would trigger LOAC requirements. Such ad hoc reasoning does little to build confidence that the international community may arrive at acceptable norms for protecting critical infrastructure from cyber threats.

Relying on self-defense as a legal justification for responding forcefully to cyber attacks would not constitute the first time that States have argued for Article 51 authority to respond with military force to a provocation that is something other than a traditional "armed attack." At least since the 1986 bombing of Libyan command and leadership targets in response to a Berlin disco bombing attributed to Libya the United States has been criticized in the international community for maintaining that it has an inherent right to use force in self-defense against acts that do not constitute a classic armed attack.[109] In addition, under the terms of the Charter, forceful responses against non-State actors are handicapped at the outset because the

106. *Id.* at 60–61.

107. An Assessment of International Legal Issues, *supra* note 52, at 19.

108. Infamously included in Justice Potter Stewart's concurring opinion in *Jacobellis v. Ohio*, where Justice Stewart concluded that he could not further define the hard-core pornography at issue in the case, "[b]ut I know it when I see it." 378 U.S. 184, 197 (1964) (Stewart, J., concurring).

109. An Assessment of International Legal Issues, *supra* note 52, at 16.

Charter was drafted to regulate relations among States. Still, for understandable reasons, States tend to defend all their uses of force as self-defense.[110] The reliance by the United States on self-defense in its targeting of terrorists outside traditional battlespaces is emblematic of the tendency to freight legally unsettled and controversial uses of force onto the Charter provision, without Security Council approval or international judicial recognition. Of course the threats to U.S. interests have been real, if unconventional, and the open-textured language of Article 51 is the single alluring source of positive law authority that may support the expansive uses of force.

However sympathetic we may be to the very real threats to national security presented by non-State terrorists wielding unconventional weapons unannounced against civilians, the Charter's role in supplying the *jus ad bellum* support for the use of force in defending against a wide range of terrorist attacks including cyber is open to question.[111] As Sean Watts has warned, over time the written law of the Charter may take a backseat to the supposed law of self-preservation.[112] At the same time, the Charter's use of force/armed attack paradigm may be construed to support justifications for self-defense actions that do more to *harm* than protect peace and security. For example, a 1999 Department of Defense Office of General Counsel assessment of information operations maintained that when a cyber attack is considered equivalent to an "armed attack," and if it is not possible or appropriate to respond by attacking the specific source of the computer attack, "any legitimate military target could be attacked . . . as long as the purpose of the attack is to dissuade the enemy from further attacks or to degrade the enemy's ability to undertake them."[113] Although such a response may be lawful under LOAC, the decision to attack "any legitimate military target" runs the risk of escalation of a non-kinetic information operation to something more lethal.

Meanwhile, it may be that the dynamic growth of reliance on the Internet to support our infrastructure and national defense has caused the United States to modify its long-standing views on the predicates for treating a cyber intrusion as an "armed attack" or "use of force." As Matt Waxman has noted, U.S. government statements may be interpreted to suggest that only cyber attacks that have especially harmful effects will be treated as

110. Watts, *supra* note 52, at 87 n.142.
111. *Id.* at 76.
112. *Id.* at 87 n.143.
113. An Assessment of International Legal Issues, *supra* note 52, at 18.

armed attacks, while lower-level intrusions would enable cyber countermeasures in self-defense.[114] If the statements represent U.S. policy, the result is a tiered interpretation of Article 51 based on the instrument of attack—an expansive interpretation when defending against armed violence and a narrower view with a high impact threshold for cyber attacks.[115] Whatever precision and calibration of authorities is gained by these fresh reinterpretations of the Charter, they replace the relative clarity of an "armed attack" criterion with fuzzier effects-based decision making that riles international lawyers and injects ever more subjectivity and less predictability into future self-defense projections. Given the characteristics of cyber war—uncertainty, secrecy and lack of attribution—finding consensus on international regulation through these Charter norms will be a tall order.[116]

As has been widely noted over the last decade or more, the Charter in general and LOAC in particular are not optimally situated in every respect to regulate conflicts between States and terrorist organizations.[117] The State-centric orientation of the international legal instruments is based on a number of fundamental conceptions that do not apply easily in asymmetric conflicts with non-State terrorists—sovereignty and borders, declarations of war or armed conflict, protections for civilians and the disincentives to attack provided by State armies and weaponry.[118] Applied to cyber war, similar features stand out. States and sovereign borders are not significant barriers to Internet-based attacks. Most cyber attackers operate anonymously and are unannounced. Their victims may be governments, businesses and/or citizens, and attribution problems and the mobility of the terrorists' base of cyber war operations nearly eliminate the disincentives to attack. There are important differences between cyber attacks and other forms of terrorism, too. For example, most terrorist attacks produce immediately observable effects of physical violence, while cyber attacks may cause harm that is not easily seen.

As applied to cyber, the critique of the United States and a few other Western States for exporting their domestic counterterrorism policies in the service of a Global War on Terror may afford an opportunity for those

114. Waxman, *supra* note 39, at 439.

115. *Id.*

116. *Id.* at 443.

117. *See* NEW BATTLEFIELDS/OLD LAWS: CRITICAL DEBATES ON ASYMMETRIC WARFARE (William C. Banks ed., 2011).

118. *Id.*

same States to have something of a "do-over" in shaping cyber defense doctrines. Unlike al Qaeda attacks directed at the United States and a few Western European allies, cyber threats are more dispersed and widespread—consider the attacks on Georgia and Estonia in recent years. In addition to the major world powers, most States have a vested interest in arriving at a set of legal norms for defending against cyber attacks. Second, the norms that a still-maturing counterterrorism law could develop for cyber defense need not be threatening to the Charter or to the rule of law generally. The often expressed criticisms of the last decade that the United States was creating law-free zones in Guantanamo Bay or through its rendition practices[119] should not prejudice the development of new cyber law. New norms could be the product of national and international strategies and policies, tested over time through State practice, and not simply derived from existing legal doctrinal categories.[120] Unlike the post-9/11 policies, new counterterrorism cyber norms would not in every instance consist of extensions of the domestic laws of sponsoring States. For example, the fact that the customary law of countermeasures does not apply to interventions by non-State actors[121] exposes a gap in international law that an emerging cyber counterterrorism law could fill. Third, because the coherence of Charter- and LOAC-based international law as applied to cyber war really is in question, the opportunity for a scheme complementary to the Charter and LOAC is upon us or will soon be so.

Most new legal fields develop in response to new social or technological phenomena. Terrorism is anything but new. To be sure, the international networking of terrorists that led to the 9/11 attacks and others since is unprecedented, but domestic and international counterterrorism has occupied government and lawmaking agendas for nearly half a century. The international law of counterterrorism has been slow to develop, largely because of the politicization of the debate over definitions of what counts as terrorism and, as a consequence, which groups and activities may be countered with government-sanctioned programs. That the field is emerging internationally, despite the continuing wrangling over definitions, reflects the realization among States and the professionals in the field that maturing

119. *See*, e.g., Leila Sadat, *Extraordinary Rendition, Torture, and Other Nightmares from the War on Terror*, 75 GEORGE WASHINGTON LAW REVIEW 1200, 1226 (2007).

120. *See* Maggs, *supra* note 75, at 704.

121. *See supra* text accompanying note 24.

domestic counterterrorism law may be exported to the international community.[122]

Attribution of cyber attacks is a technical problem, not one that the law can fix. Yet the challenges in attributing intrusions in real time with confidence should not foreclose the development of legal authorities that can support responses that protect national and human security. Anonymity and surprise have long been central tenets of terrorist attacks, and counterterrorism law has developed normative principles—such as anticipatory self-defense—that accommodate these characteristics. By analogy counterterrorism law can develop along similar lines to provide *ad bellum* bases for responding to cyber attacks. In light of continuing attribution problems, and the likelihood that cyber attacks will come from sources around the world, a cyber counterterrorism law could subordinate traditional legal protections that attach to national boundaries and narrowly tailor mechanisms that permit defending against the sources of the attacks, whatever their locations. One of the difficulties of attribution is that learning that an attack comes from within a certain State does not tell us whether the attack is State-sponsored or was done by a non-State actor. Because existing Charter and LOAC law of State responsibility—heavily influenced by the United States and other Western States that do not have comprehensive controls over private infrastructure—does not make the State responsible for the actions of private actors over which it has no direction or control, there is no clear LOAC- or Charter-based authority to go after the private attackers inside a State when that State was not involved in the attacks.[123] Counterterrorism law offers an alternative normative path, if criteria can be developed that tell decision makers when absolute attribution may be delayed in favor of immediate defensive action, when intelligence is reliable enough to authorize those actions and under which circumstances defensive operations may invade territorial sovereignty without State permission.[124] The analogies to ongoing U.S. actions in its counterterrorism targeting program are striking.[125]

---

122. *See* Moeckli, *supra* note 71, at 173, 176–77; *see generally* GLOBAL ANTI-TERRORISM LAW AND POLICY, *supra* note 76.

123. *See* TALLINN MANUAL, *supra* note 13, rule 6.

124. The policy decision in such an instance may be based on different factors, of course, and may lead to decisions not to intervene where the law would permit the operation.

125. *See* Robert M. Chesney, *Who May Be Killed? Anwar al-Awlaki as a Case Study in the International Legal Regulation of Lethal Force*, 13 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 3 (2011).

Just as counterterrorism law is developing through an uneven process of fits and starts, missteps and recalibrations, it is likely that international law governing cyber war will emerge in a similar way, over time, as the product of State, regional and perhaps even global policies and strategies. First-generation counterterrorism law developed by analogy to decades of armed violence in the proxy wars fought during the Cold War. Secrecy was the norm, attribution was unofficial or non-existent and the *jus ad bellum* architecture was unclear at best. Indeed, controversy continues to surround State practice in certain counterterrorism policies, such as the shadow war being waged by the United States against al Qaeda and its affiliates in more than a dozen countries outside traditional battlespaces.[126]

Second-generation counterterrorism law is evolving now, a combination of exported second-generation domestic counterterrorism laws, some pertinent international treaties, bi- and multilateral agreements, and State practices that are maturing in responding to al Qaeda and other terrorist groups. Lessons have been learned from the proxy wars experience and from responding to terrorist attacks. Because terrorists' lack of attribution and surprise tactics require high levels of operational secrecy in counterterrorism, domestic legal reforms have moved toward greater regulation of intelligence operations, emphasizing the providing of information on intelligence operations to overseers, and an emphasis on positive identification of targets in potentially lethal counterterrorism operations.[127]

Intelligence collection is practiced by every State. While the domestic laws of nearly every State forbid spying within its territory, neither those laws nor any international law purports to regulate espionage internationally. The growing capabilities for cyber sleuthing in the digital age suggest that development of a cyber-based intelligence law from a counterterrorism platform may be an important component of the architecture for twenty-first-century cyber war governance. In the digital world, the equivalent intelligence collection activity is cyber exploitation—espionage by computer, a keystroke monitor, for example—and nothing in the Charter, LOAC or customary law would stand in its way, except to the extent that espionage

126. Scott Shane, Mark Mazzetti & Robert F. Worth, *Secret Assault on Terrorism Widens on Two Continents*, NEW YORK TIMES (Aug. 14, 2010), http://www.nytimes.com/2010/08/15/world/15shadowwar.html?pagewanted=all&_r=0.

127. *See* William C. Banks, *The United States a Decade After 9/11*, *in* GLOBAL ANTI-TERRORISM LAW AND POLICY, *supra* note 76, at 449, 450–51, 470–80.

involving military weapons systems constitutes armed aggression.[128] Given the growing capabilities of digital devices to spy, exploit and steal, including military and other sensitive national secrets, the absence of international regulation is striking and troubling. It is possible that LOAC could develop customarily to recognize legal limits on cyber exploitation where the software agent is capable of destructive action or may facilitate the same.[129] Yet intelligence collection is also at the center of counterterrorism, and likewise is subject to domestic legal controls, but no international legal regulation. As cyber exploitation assumes an ever more important role in States' cyber defenses, might the international community consider developing some regulatory principles as part of counterterrorism law?

In the intelligence regulation respect and others counterterrorism law for cyber operations may evolve through something like natural law–type or just war theory reasoning, as has been the case with the development of some other international law norms.[130] Just war theory and natural law reasoning or its equivalent has served as a gap filler in international law, and could do so for cyber. Like counterterrorism law as developed and exported by the United States after 9/11, the making of customary international law is often unilateral in the beginning, followed by a sort of dialectic of claims and counterclaims that eventually produce customary law that is practiced by States.[131] Ironically, as some prominent U.S. academics developed theories of "vertical domestication"[132] to encourage greater respect and adherence to international law by the U.S. government, in the last decade the U.S. government sought to export its emerging counterterrorism law as international law in response to kinetic attacks on the United States and its interests. Although controversy surrounded some of the U.S. government policies and practices, counterterrorism law has matured and developed normative content around some of its revised tenets, such as mili-

128. *See* Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 AIR FORCE LAW REVIEW 217, 223–24 (1999).

129. *See* TECHNOLOGY, POLICY, LAW, AND ETHICS, *supra* note 22, at 261, 263.

130. *See* Jeffrey L. Dunoff & Mark A. Pollack, *What Can International Relations Learn from International Law?* 11 (Temple University Legal Studies Research Paper No. 2012-14, 2012), http://ssrn.com/abstract=2037299.

131. See the description of the process in W. Michael Reisman, *Assessing Claims to Revise the Laws of War*, 97 AMERICAN JOURNAL OF INTERNATIONAL LAW 82 (2003).

132. Harold Hongju Koh, *The 1998 Frankel Lecture: Bringing International Law Home*, 35 HOUSTON LAW REVIEW 623, 626–27 (1998) (citing Harold Hongju Koh, *Transnational Legal Process*, 75 NEBRASKA LAW REVIEW 181, 183–84 (1996)).

tary detention and the use of military commissions.[133] Other States may develop counterterrorism legal authorities in this emerging paradigm of cyber war through a similar process.

However it occurs, counterterrorism law norm development for cyber might expand or contract the authorities that would otherwise govern under current interpretations of the Charter. On the one hand, an evolving counterterrorism law regime may enable victim States with more tools and greater flexibility in anticipating and responding to cyber attacks. Active defense countermeasures and other kinds of responses may be permitted through State practice, but predicated upon counterterrorism authority, where the same responses would not have been lawful under the Charter as traditionally interpreted because the armed attack threshold was not met. On the other hand, some cyber responses that are now lawful under international law because there is no use of force or armed attack involved in the response—a small scale action designed to neutralize an incoming cyber intrusion aimed at one system, for example—could be considered unlawful if the harmful consequences are significant.[134]

For the United States, the fact that so much of our infrastructure is privately owned makes securing the infrastructure legally and practically problematic,[135] yet our heavy reliance on networked information technology makes us highly vulnerable to cyber intrusions. Our government's recent posture on cyber operations has been to mark out preferred clear positions on the authority to respond to destructive cyber attacks with armed or forceful responses, while maintaining what Matt Waxman aptly calls "some permissive haziness"[136] concerning the norms for responding to cyber intrusions that are less harmful but distracting. From the domestic perspective, the United States can assure itself of the authority to respond to serious intrusions, while preserving the flexibility to tailor its countermeasures and develop its cyber defenses according to the nature and severity of the threat faced.

The nuanced calculations by the United States in developing its cyber doctrine is consistent with its long-standing opposition to some other States' expansive interpretations of Articles 2(4) and 51 to include econom-

133. Banks, *supra* note 127, at 478–80; Robert M. Chesney, *Who May Be Held? Military Detention Through the Habeas Lens*, 52 BOSTON COLLEGE LAW REVIEW 769 (2011).

134. TECHNOLOGY, POLICY, LAW, AND ETHICS, *supra* note 22, at 245.

135. Waxman, *supra* note 39, at 451.

136. *Id.* at 452.

ic coercion and political subversion.[137] Yet emerging cyber doctrine by the United States may be seen in the international community as just the sort of proposed expansion of the Charter norms that the United States has publicly opposed in the past. Indeed, as the evolving criteria for what triggers the Article 51 right of self-defense over the last twenty-five years show, freighting fast-developing cyber defense norms onto an already burdened Article 51 invites controversy and may destabilize and even undermine the normative value of the Charter.

Developing cyber doctrine may be more effective and more likely to be accepted internationally if it is separated from the effects-based approach relied upon by the Charter and LOAC-based doctrines for cyber operations. Relying on a developing counterterrorism law to embody the cyber doctrines internationally would thus serve the ancillary goal of retaining the traditional military force core of the bookend Charter provisions. Not that such a legal code of conduct based in counterterrorism law would be a panacea. Law must follow, not lead, particularly in an area like cyber, where policies are not yet well defined and strategies are unclear.[138]

National policies and operational practices will lead us toward a supplemental cyber law. Consider an illustration from counterterrorism law that developed in the carrying out of kinetic operations by the U.S. military in recent years when U.S. forces pursue a lawful target in a counterterrorism operation. As highlighted by the raid that killed Osama bin Laden in 2011, the operational standard includes a "kill or capture" option, deferring to commanders on when a capture may reasonably be accomplished. Under the Charter and LOAC, once a lawful target has been positively identified, the use of lethal force without further deliberation is lawful. The theoretically more human rights–oriented operational law, driven by counterterrorism policy, is becoming part of international counterterrorism law through State practice. In fact, operational law and military service lawyers have taken on a central role in military decision making and thus in the shaping of State practice, especially after 9/11.[139] Cyber law in counterterrorism may develop in much the same way, based on operational rules and State practice that tailor the legal norms to requirements.[140]

---

137. *Id.* at 453.

138. *Id.* at 455–57.

139. *See* JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11, at 122–60 (2012).

140. *See* Ian Hurd, *Is Humanitarian Intervention Legal? The Rule of Law in an Incoherent World*, 25 ETHICS AND INTERNATIONAL AFFAIRS 293 (2011) (noting the dynamic relation-

V. CONCLUSIONS

Imagine one more scenario. This one takes place during summertime in the not-distant future. Just before the afternoon rush hour on a hot and steamy July day, the northeastern United States is hit with a massive blackout. The electric grid is crippled from Boston to New York, Philadelphia to Baltimore and Washington, and from there west as far as Cleveland. While backup generators resume the most critical operations in hospitals and other critical care centers, all other activities that depend on electricity come to a sudden halt.

Government and private industrial security experts quickly discover the software and malware that has accessed supervisory control and data acquisition (SCADA) controls—the industrial control system that supervises data over dispersed components of the electric grid and which are connected to the global Internet.[141] In recent years, industry reports that a few laptops containing information on how to access SCADA controls were stolen from utility companies in the Midwest. During the same period, computers seized from al Qaeda captives contained similar details about U.S. SCADA systems. The vast majority of the affected electric grid is privately owned, and officials estimate that the cyber attacks have done long-term damage to critical system components, and have rendered useless generators and other equipment that must be replaced where no backup replacement equipment is standing by. Even rudimentary repairs will take weeks or months, and full system capabilities may not be restored for more than one year. Economic losses will be in the billions of dollars, and millions of Americans' lives will be disrupted for a long time.

The software and malware were set to trigger the blackout at a predetermined time. The attacks were not attributed, and although intelligence and law enforcement experts quickly traced the original dissemination of the attacks to computers in South Asia, the only other available intelligence comes from the seized and stolen laptops mentioned above. The governments of Russia, China and Iran have denied any involvement in the attacks, and no intelligence points to their involvement. Al Qaeda has shown interest in cyber war capabilities, and the seized laptops suggest that some steps were taken to acquire them.

---

ship between State practice and international law where humanitarian intervention may be legally plausible despite Article 2(4)).

141. *See* BRENNER, *supra* note 3, at 96–97 (describing SCADA systems).

Assuming that the United States concludes that al Qaeda is most likely behind the attacks, what law governs the response? If, instead, we decide that the attacks were launched by Russian intelligence operatives situated in South Asia, what law governs the response? This article has helped draw attention to the incompleteness of the legal regime that will be required to provide the normative justifications for responding to these intrusions.

The stakes are escalating. The United States used offensive cyber weapons with Stuxnet to target Iran's nuclear program, and nation States and non-State actors are aware that cyber warfare—offensive and defensive—has arrived with growing sophistication. Although reports indicated the United States declined to use cyber weapons to disrupt and disable the Qaddafi government's air defense system in Libya at the start of the U.S./NATO military operation in 2011 because of the fear that such a cyber attack might set a precedent for other nations to carry out their own offensive cyber attacks,[142] Stuxnet created the precedent, as did Israel's cyber attack on Syrian air defenses when it attacked a suspected Syrian nuclear site in 2007,[143] Russia's cyber attacks in its dispute with Georgia[144] and the apparent use of cyber weapons by the United States to target al Qaeda websites and terrorists' cell phones.[145] Now that the cyber war battlefield apparently has expanded to Beirut banks and a neutral State,[146] it appears that cyber weapons are being used beyond countering imminent national security and infrastructure threats.

Developing an international consensus on the norms for cyber war will be especially difficult, particularly in determining what kinds of cyber attacks trigger the authority to take defensive actions and the nature of the defenses that will be permitted. The facts needed to make the normative

142. Eric Schmitt & Thom Shanker, *U.S. Debated Cyberwarfare in Attack Plan on Libya*, NEW YORK TIMES (Oct. 17, 2011), http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

143. David A. Fulghum, Robert Wall & Amy Butler, *Cyber-Combat's First Shot: Attack on Syria Shows Israel is Master of the High-Tech Battle,* AVIATION WEEK & SPACE TECHNOLOGY, Nov. 26, 2007, at 28.

144. John Markoff, *Before the Gunfire, Cyberattacks*, NEW YORK TIMES, Aug. 12, 2008, at A1.

145. *See supra* notes 11–12; Jack Goldsmith, *Quick Thoughts on the USG's Refusal to Use Cyberattacks in Libya*, LAWFARE (Oct. 18, 2011, 7:48 AM), http://www.lawfareblog.com/2011/10/quick-thoughts-on-the-aborted-u-s-cyberattacks-on-libya/.

146. Katherine Mayer, *Did the Bounds of Cyber War Just Expand to Banks and Neutral States?*, THE ATLANTIC, Aug. 21, 2012, http://www.theatlantic.com/international/archive/2012/08/did-the-bounds-of-cyber-war-just-expand-to-banks-and-neutral-states/261230/#.UDPjrcFCPJo.email.

judgments in this fast-paced realm of changing technologies are now and will be for the foreseeable future hard to come by and even more difficult to verify.[147] Law will play catch-up, as it should, but the lag between evolving technologies and normative stability in cyber operations may be a long one.

This article has shown that the international community in general and the United States in particular run some significant risks by continuing to build cyber war law using the Charter/LOAC model. One overarching concern is that categorizing cyber attacks as a form of armed attack or use of force may enhance the chance that a cyber exchange could escalate to a military conflict.[148] If, over time, the thresholds for what constitutes an armed attack are lowered to reach more forms of cyber attack, legal barriers to military force will be lowered at the same time, leading to more military conflicts in more places. The high threshold for invoking the Charter's self-defense authorities traditionally supported by the United States also offers some insurance against precipitous action in response to unattributed cyber attacks. That such a high threshold fails to deter low-level hostilities may be a reasonable price to pay.[149]

Yet the high self-defense threshold also leaves unregulated (at least by the Charter and LOAC) a wide swath of cyber intrusion techniques, those now in existence and others yet to be invented. This by product of the bifurcation of international law into war and peace, armed conflict or not armed conflict, armed attack and use of force or not leaves every intrusion that fails to meet the kinetic standard not subject to international law limitations, except for the limited customary authorities for countermeasures and the open-ended rule of necessity.[150] If States or the international community attempts to further expand the reach of self-defense and LOAC in idiosyncratic ways to non-destructive cyber intrusions, the Charter and LOAC will be compromised.

The effects-based approach to interpreting the Charter and LOAC in the cyber realm tends toward incoherence and lacks a normative core. Counterterrorism law could support or help build the normative architecture for cyber operations, at least at the margins, where the legal landscape

147. *See* Waxman, *supra* note 39, at 448.

148. MARTIN C. LIBICKI, CYBERDETERRENCE AND CYBERWAR 69–70 (2009); O'Connell, *supra* note 20.

149. *See* Waxman, *supra* note 39, at 446–47.

150. *See* TALLINN MANUAL, *supra* note 13, rule 9, cmts. 10 & 12 (reviewing the "plea of necessity" recognized in Article 25 of the Articles on State Responsibility).

is not now clear. Over time a cyber regime may develop that supplements the Charter and LOAC and permits forceful responses to especially destructive intrusions while preserving some yet-to-be-defined lower-intensity options for less harmful attacks.

More particularly, despite the disconnect between the text of the Charter as interpreted by the ICJ and State practice, whether an attack is kinetic or cyber-based, State practice has been to enable armed force in response to an imminent attack if it reasonably appears that a failure to act promptly will deprive the victim State of the opportunity to defend itself. Article 51, or at least its self-defense shadow, has become the go-to authority for military action waged by States, whatever the context. The self-defense arguments may be and have been adapted to cyber, but the further the analogies to responses to armed attacks stray from kinetic means, the greater the likelihood that Article 51 norms will erode. The temptation to rely on Article 51 is great, to be sure, particularly where, as in cyber, other sources of legal authority to take what is viewed as essential defensive action may not exist.

The Charter- and LOAC-based cyber law that has developed in fits and starts over recent decades is reminiscent of the adage that if you only have a hammer, you see every problem as a nail. We have invested in military capabilities for cyber, so it has become a military use of force legal problem.[151] The Charter and LOAC do not have all the answers, and cyber is not fundamentally a military problem.

151. I am indebted to General Ken Watkin, Canadian Forces (Ret.), for reminding me of the relevance of the adage.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Cyber Attacks: Proportionality and Precautions in Attack

Eric Talbot Jensen

89 INT'L L. STUD. 198 (2013)

Volume 89 2013

Cyber Attacks: Proportionality and Precautions in Attack

Eric Talbot Jensen[*]

I. INTRODUCTION

When David Sanger[1] and Ellen Nakashima[2] officially broke the news that the United States and Israel had been involved in a long-term collaborative cyber operation focused on Iran and its nuclear development capabilities, they only confirmed what many had assumed for some time.[3] In

* Associate Professor, Brigham Young University Law School. The author wishes to thank Brooke Robinson and Brigham Udall for their exceptional research assistance.

1. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES, June 1, 2012, at A1, *available at* http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0; *see also* DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER (2012).

2. Ellen Nakashima, Greg Miller & Julie Tate, *U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say*, WASHINGTON POST (June 19, 2012), http://articles.washingtonpost.com/2012-06-19/world/35460741_1_stuxnet-computer-virus-malware.

3. William J. Broad, John Markoff & David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, NEW YORK TIMES, Jan. 15, 2011, at A1, *available at* http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html; Tucker Reals, *Stuxnet Worm a U.S. Cyber-Attack on Iran Nukes?*, CBS NEWS (Sept. 24, 2010, 6:41 AM), http://www.cbsnews.com/8301-501465_162-20017507-501465.html; *A worm in the centri-*

fact, with the discovery of Stuxnet in 2010, many scholars and practitioners had speculated on whether the use of the Stuxnet malware, if State sponsored, amounted to a "use of force" or even an "armed attack" under the UN Charter paradigm.[4]

Some even began to consider the hypothetical legality of Stuxnet-type cyber actions within an armed conflict as opposed to a use of force or armed attack that would initiate an armed conflict. For these writers, the major issues revolved around the cyber tool's compliance with the law of armed conflict (LOAC) and principles such as discrimination and proportionality. For example, Jeremy Richmond analyzed Stuxnet in light of these principles and concluded that whoever designed the malware did so with the clear intent to comply with the LOAC.[5]

Even prior to the discovery of Stuxnet, a group of legal and technical experts[6] were gathered by the Estonian Cooperative Cyber Defence Centre of Excellence to draft a manual, known as the *Tallinn Manual on the International Law Applicable to Cyber Warfare*.[7] The *Manual* explores the international law governing the use of force—in both its *jus ad bellum* and *jus in bello* aspects[8]—as applied to cyber operations conducted by States and non-State actors. Several key principles arose during the *Manual* discussions in relation to the principles of proportionality and precautions in and against attack, including a number of challenging aspects in applying these principles

---

fuge, ECONOMIST, Oct. 2, 2010, at 63, *available at* http://www.economist.com/node/17147818.

4. Gary D. Brown, *Why Iran Didn't Admit Stuxnet Was an Attack*, JOINT FORCE QUARTERLY, Oct. 2011, at 70, *available at* http://www.ndu.edu/press/lib/images/jfq-63/JFQ63_70-73_Brown.pdf; Chance Cammack, Comment, *The Stuxnet Worm and Potential Prosecution by the International Criminal Court Under the Newly Defined Crime of Aggression*, 20 TULANE JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW 303, 320–23 (2011); John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, 29 JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 1, 9–11 (2011).

5. Jeremy Richmond, Note, *Evolving Battlefields: Does STUXNET Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INTERNATIONAL LAW JOURNAL 842, 883–93 (2012).

6. The author was a member of the group.

7. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

8. The *jus ad bellum* regulates the laws of conflict management, or the laws governing going to war. The *jus in bello* regulates activities once armed conflict has begun. Though some terms are similar in both bodies of law, they are considered separate and distinct under the current armed conflict paradigm.

to cyber warfare. This article will discuss some of those interesting challenges.

Part II of the article will focus on the constant-care standard and how it applies to all cyber operations. Part III will look at the principle of proportionality with specific focus on the idea of indirect effects. Part IV analyzes the issue of feasibility with the precautionary standards. Part V analyzes State responsibilities under the obligation to take precautions against the effects of attacks. The article will conclude in Part VI.

A. Attack

Before embarkation on the above-mentioned analysis, some brief comments are necessary concerning the definition of "attack." With the exception of Part II, which deals with the constant-care standard, the legal standards discussed below apply to an "attack." Many LOAC principles apply only to situations of attack, such as the principle of proportionality. The idea of taking precautions in the attack assumes that there is an attack. The fundamental nature of "attack" underlies many of the LOAC principles that govern cyber warfare, making it important to come to some understanding of the meaning of the word.

Paul Walker was one of the first to address this issue directly, in his article "Rethinking Computer Network 'Attack.'"[9] He notes that the word "attack" is defined in the 1977 Additional Protocol I (API) to the Geneva Conventions as "acts of violence" and states that this definition has become customarily binding even on non-parties to the Protocol.[10] As a result, Walker argues that very few activities in cyber warfare will actually amount to an attack and will therefore not be governed by the principles of attack, such as proportionality.

The meaning of "attack" was also vigorously debated by Michael Schmitt,[11] Chairman of the International Law Department of the U.S. Naval War College and leader of the *Tallinn Manual* project, and Knut Dörmann, representative of the International Committee of the Red Cross

9. Paul A. Walker, *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*, 1 NATIONAL SECURITY LAW BRIEF 33 (2011), *available at* http://digitalcommons.wcl.american.edu/nslb/vol1/iss1/3.

10. *Id.* at 34.

11. Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 84 INTERNATIONAL REVIEW OF THE RED CROSS 365, 374–79 (2002), *available at* http://www.icrc.org/eng/assets/files/other/365_400_schmitt.pdf.

(ICRC).[12] In Schmitt's view, an attack is something that results in death, damage, destruction or injury. Dörmann argued that anything that was aimed at civilians amounted to an "attack." These views tend to mark the extremes of the debate. The *Tallinn Manual* softened Schmitt's view somewhat by indicating that a cyber attack need not be characterized by the release of kinetic force.[13]

Resolving the debate on the definition of attack may need to wait for more State practice. It is enough for this article to state that most of the law discussed here presupposes an "attack," whatever that means. For example, in the absence of an attack, commanders are not required to apply the principle of proportionality.

B. State and Non-State Actors

In addition to the definition of "attack," another important consideration is the involvement of non-State actors in cyber operations. One of the most intriguing aspects of cyber operations is that they allow non-State actors to relatively easily harness State-level violence. This undermines the Westphalian monopoly on the use of violence as few other weapon systems have done.

Other articles in this volume will address this question more directly,[14] so little need be said here except to note that many of the standards discussed below only apply to States. To the extent that some organized armed groups might elect to be bound by LOAC principles, they would also be bound, but as a matter of law the majority of the discussion below applies to States.

12. KNUT DÖRMANN, APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS (2004), *available at* http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf; Knut Dörmann, *The legal situation of "unlawful/unprivileged combatants,"* 85 INTERNATIONAL REVIEW OF THE RED CROSS 45, 46, 72–73 (2003), *available at* http://www.icrc.org/eng/assets/files/other/irrc_849_ dorman.pdf.

13. TALLINN MANUAL, *supra* note 7, rule 30.

14. For example, Michael Schmitt's article on the application of these principles to non-international armed conflict discusses non-State actors. Michael Schmitt, *Classification of Cyber Conflict*, 89 INTERNATIONAL LAW STUDIES ___ (forthcoming 2013).

II. THE "CONSTANT-CARE" STANDARD

Article 57 of Additional Protocol I is titled "Precautions in the Attack"[15] and is generally believed to be binding on States in both international armed conflict and non-international armed conflict.[16] However, the first subparagraph takes a much broader approach than just "attack." It states that "[i]n the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects."[17] The ICRC *Commentary* adds, "The term 'military operations' should be understood to mean any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat."[18]

The term "military operations" is obviously meant to be much broader than the term "attack" and imposes a general legal requirement on militaries even when not attacking. The legal requirement is to exercise "constant-care," but that term is not defined either in Article 57, the ICRC *Commentary* or generally in the LOAC. While the exact application of this principle in a specific military operation must be left to the commander, it seems clear that exercising constant care would at least mean that a commander cannot ignore effects on civilian population.

In the context of cyber operations, constant care would likely require a commander to maintain situational awareness at all times, including all

---

15. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 57, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter API].

16. TALLINN MANUAL, *supra* note 7, rule 52; 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW rule 15, at 51 (Jean-Marie Henchaerts & Louise Doswald-Beck eds., 2005) [hereinafter ICRC CIL STUDY]; MICHAEL N. SCHMITT, CHARLES H.B. GARRAWAY & YORAM DINSTEIN, THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT WITH COMMENTARY ¶ 2.1.2 (2006), *reprinted in* 36 ISRAEL YEARBOOK ON HUMAN RIGHTS (special supplement) (Yoram Dinstein & Fania Domb eds., 2006) [hereinafter NIAC MANUAL]; U.S. Navy, U.S. Marine Corps & U.S. Coast Guard, NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7A, The Commander's Handbook on the Law of Naval Operations ¶ 8.1 (2007), *available at* http://www.usnwc.edu/getattachment/a9b8e92d-2c8d-4779-9925-0defea93325c/1-4M_(Jul_2007)_(NWP [hereinafter Commander's Handbook]; UNITED KINGDOM MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 5.32 (2004) [hereinafter UK MANUAL]; COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 680 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987) [hereinafter API COMMENTARY]. *See also id.* at 600 (explanation of the term "operations").

17. API, *supra* note 15, art. 57.1.

18. API COMMENTARY, *supra* note 16, at 680.

phases of the operation. When employing a cyber tool or conducting cyber operations, the commander would need to maintain oversight of the tool and be ready to adjust operations if the tool or operation began to have effects that the commander determined would have an illegal impact on civilians. This might be especially difficult in the cyber domain since virtually every cyber operation will traverse, affect, employ or damage civilian cyber infrastructure of some kind.[19]

A contemporary application of this standard occurred in the case of the infamous Stuxnet malware.[20] Evidently, it was discretely targeted at Iranian nuclear facilities, but reports show that it spread much wider than that, presumably wider than the United States and Israel[21] intended it to disseminate, which may have led to its discovery. Though no other damage was reported, the unintended spread of the virus at least implicates the constant-care standard and informs State practice on the issue.

Additionally, it appears that the Stuxnet malware was used in conjunction with another malware that has been termed "Flame." Flame was "designed to secretly map Iran's computer networks and monitor the computers of Iranian officials, sending back a steady stream of intelligence used to enable an ongoing cyberwarfare campaign."[22] Flame was discovered by Iranian officials when Israeli government hackers were carrying out operations against Iranian oil ministry and export facilities.[23]

Similar situations might lead a commander to argue that he cannot continue to monitor the network in order to exercise constant care for fear of being discovered. The LOAC allows no such exception in this case, though it does in others.[24] Therefore, it seems unlikely that a commander could

---

19. Michael McConnell, Former Director of National Intelligence, Keynote Address at the Texas Law Review Symposium: Law at the Intersection of National Security, Privacy, and Technology (Feb. 4, 2010) [hereinafter McConnell], *referred to in* Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks,* 88 TEXAS LAW REVIEW 1533, 1534 (2010).

20. Nicolas Falliere, Liam O Murchu & Eric Chien, W32.Stuxnet Dossier, Version 1.4, (Feb. 2011), http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

21. Sanger, *supra* note 1.

22. Nakashima, Miller & Tate, *supra* note 2.

23. *Id.*

24. For example, the Hague rules require the attacker to "do all in his power to warn the authorities" unless the attack is an "assault." Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. IV Respecting the Laws and Customs of War on Land art. 26, Oct. 18, 1907, 36 Stat. 2227, *available at* http://www.icrc.org/ihl.nsf/FULL/195?OpenDocument; *see also* TALLINN MANUAL, *supra* note 7, rule 58.

argue that he was relieved of his legal duty to maintain constant care for fear it might lead to discovery. Rather, commanders and all persons conducting cyber operations must recognize and accept the legal obligation to exercise constant care in all military operations, including cyber operations.

III. PROPORTIONALITY AND INDIRECT EFFECTS

The principle of proportionality is found in Article 51(5)(b) of API:[25]

> 5. Among others, the following types of attacks are to be considered as indiscriminate:
>
> . . .
>
> (b) an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.

This principle is generally accepted as customary international law in international and non-international armed conflicts and is analyzed elsewhere in great length[26] so it needs no further discussion here.

Few would argue that the principle of proportionality does not apply to cyber warfare; instead the controversy centers on its application to specific cyber operations.[27] While all cyber operations are governed by the constant-care standard, the principle of proportionality will only apply to those cyber operations that amount to an "attack." For those operations where the principle of proportionality does apply, two specific aspects of the rule deserve more detailed analysis: the understanding of "damage" and the problem of indirect effects.

---

25. *See also* Amended Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices art. 3(3), May 3, 1996, 2048 U.N.T.S. 93, 1342 U.N.T.S. 168; Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict art. 7, Mar. 26, 1999, 2253 U.N.T.S. 212.

26. *See, e.g.*, Eric Talbot Jensen, *Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AMERICAN UNIVERSITY INTERNATIONAL LAW REVIEW 1145, 1170–75 (2003); Richmond, *supra* note 5, at 889–93.

27. *See generally* TALLINN MANUAL, *supra* note 7, rule 51 (discussing the application of proportionality to cyber warfare).

Preliminarily, it is important to keep in mind that civilians can never be made the object of attack[28] and that the principle of proportionality limits commanders when, as the result of a lawful attack, civilians or civilian objects may be harmed. In order for such an attack to be lawful, the commander must determine that the death, injury and damage are not "excessive in relation to the concrete and direct military advantage anticipated." Though cyber attacks will inevitably have the ability to kill and injure civilians, the vast majority of known cyber operations have focused on or resulted in damage, hence the focus on the damage element of the legal standard.

Additionally, the requirement that the damage occur to civilian objects should be understood broadly. The vast majority of the Internet, including the cables, servers and routers, consists of civilian objects, which are owned, operated and maintained by civilians. Any damage to these elements of the Internet infrastructure would be considered civilian damage for purposes of the proportionality analysis.

Finally, although the drafters of 1977 Additional Protocol I certainly did not anticipate cyber warfare, they did recognize that electronic advances in technology would affect the way wars would be fought and their potential impacts on civilians. In the *Commentary*, the ICRC notes, "It was also pointed out that modern electronic means made it possible to locate military objectives, but that they did not provide information on the presence of civilian elements within or in the vicinity of such objectives."[29] Though perhaps not entirely true in cyber warfare, this idea certainly impacts the application of proportionality to cyber attacks.

A. Damage to Civilian Objects

When considering kinetic weapons that result in heat, blast and fragmentation, the issue of defining damage is less controversial. However, when cyber tools are used to conduct an attack, determining what cyber actions amount to damage becomes more problematic. There are several approaches in determining what equates to damage in the cyber domain.

One approach would be to analogize from a kinetic attack and argue that if what occurs from a cyber operation would have been considered damage if accomplished by kinetic means, then the attack amounts to dam-

28. API, *supra* note 15, art. 48.

29. API COMMENTARY, *supra* note 16, at 625.

age. The advantage to this approach is that it places commanders in a comfortable position to apply known factors. Commanders have been applying the proportionality analysis to kinetic attacks their entire careers and will likely feel quite comfortable with this analysis.

However, there are many cyber actions that would not look at all like the results of a kinetic attack. For example, simply closing a computer's specific communication port normally used to communicate with another computer, while leaving the rest of the computer function untouched, is not a similar effect to what might be caused by a kinetic attack. Using the kinetic analogy approach, an extremely limited number of cyber attacks would cause damage.

Alternatively, one could take the view that any unauthorized intrusion into a computer or computer system results in a change to the computer or system and therefore equates to damage.[30] In other words, the digital changes required to allow penetration into a computer would be damage under the principle of proportionality. This view would require a commander to essentially consider any effects on a computer system in his proportionality analysis.

This seems to go too far. The principle of proportionality was clearly not designed to exclude the possibility of any civilian casualties or damage, but only that which was excessive.[31]

Finally, some have taken the view that damage also encompasses serious interruptions in functionality, such as would require replacing parts or reloading software systems. For example, in the kinetic analogy used above where a cyber attack shut down a communication port but left the rest of the computer unaffected, the computer would still turn on but its actual functionality might be seriously affected. If functionality is considered when determining damage, the kinetic analogy would be of limited value.

---

30. WALTER GARY SHARP SR., CYBERSPACE AND THE USE OF FORCE 140 (1999) (where the author argues that "any computer network attack that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force that may constitute an armed attack prompting the right to self-defense"); TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 253–54 (William A. Owens, Kenneth W. Dam & Herbert S. Lin eds., 2009) (which states "actions that significantly interfere with the functionality of that infrastructure can reasonably be regarded as uses of force, whether or not they cause immediate physical damage").

31. Walter Gary Sharp Sr., *Operation Allied Force: Reviewing the Lawfulness of Nato's Use of Military Force to Defend Kosovo*, 23 MARYLAND JOURNAL OF INTERNATIONAL LAW AND TRADE 295, 313 (1999); *see also* Commander's Handbook, *supra* note 16, ¶ 8.1.2.1.

The functionality approach seems to be the best application of the proportionality rule to the cyber realm as it takes into account the unique aspects of cyber operations, without going so far as to make the proportionality analysis unwieldy for commanders to apply. Armed conflict has always included effects on civilians that have caused inconvenience, irritation, stress and fear, but these have traditionally not been part of the commander's analysis of damage required by the proportionality analysis.[32] By focusing on functionality, the commanders can easily understand the legal standard and apply it to modern cyber operations.

B. Indirect Effects

Gauging indirect effects in cyber warfare may prove to be one of the most difficult issues in applying proportionality. It is clear that a commander must consider the direct effects of his cyber attack. These direct effects are defined as the "immediate, first order consequences, unaltered by intervening events or mechanisms."[33] In the cyber domain, this would include the effects on a computer that is shut down by a cyber attack or the damage to the centrifuges caused by the Stuxnet malware.

In contrast to direct effects, indirect effects are "the delayed and/or displaced second-, third-, and higher-order consequences of action, created through intermediate events or mechanisms."[34] In the cyber domain, this would include damage that was not the intent of the attack, but that resulted from elements of the attack. In the case of Stuxnet, the malware infected many computers beyond its intended targets within Iran. Whatever damage might have resulted from these unintended infections might have been indirect effects. Another example might be a targeted attack on a military computer system that would shut the system down, but, because of the linkages between military and civilian systems, the malware is also likely to spread to the civilian systems and shut them down as well. Resulting indi-

32. Geoffrey S. Corn & Gary P. Corn, *The Law of Operational Targeting: Viewing the LOAC Through an Operational Lens*, 47 TEXAS INTERNATIONAL LAW JOURNAL 337, 364–66 (2012); Jensen, *supra* note 26, at 1170–71; Michael N. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance*, 50 VIRGINIA JOURNAL OF INTERNATIONAL LAW 795, 826 (2010).

33. Chairman, Joint Chiefs of Staff, Joint Publication 3-60: Joint Targeting, at I-10 (2007), *available at* http://www.bits.de/NRANEU/others/jp-doctrine/jp3_60(07).pdf.

34. *Id.*

rect effects are generally accepted as being included in the proportionality analysis.[35]

Even in the cases mentioned above, for the damage to be considered in the proportionality analysis, it must have been expected. Indirect effects which were not expected to be excessive are not factored into the analysis.[36] In other words, this standard does not anticipate that a reviewer can come after the fact and assess the reasonableness of the commander's decision on the excessiveness of the indirect effects. Rather, any reviewer must assess the reasonableness of the commander's decision based on what the commander reasonably expected the effects to be, given the information he had at the time.[37]

Considerations of expected effects have already affected known military operations. In the 2003 U.S. attacks on Iraq, cyber attackers for the United States considered attacking Saddam Hussein's financial accounts in an attempt to pressure him. The attacks were called off, however, when it was determined that the attacks would probably affect the European banking system and have negative repercussions.[38]

Similar considerations would have to be made in the case that a prospective malware targeting military objectives was to be implemented via a portable storage device. The commander would have to determine whether or not the potential transfer of that same malware to civilian systems was expected, and then consider how much damage it was expected to cause. On the other hand, if that same malware was unexpectedly transferred into civilian systems, the commander would not be responsible for having misapplied the principle of proportionality.

A commander's ability to properly apply this rule is obviously tied back to the earlier discussion on constant care. Unless a commander is constant-

35. Commander's Handbook, *supra* note 16, ¶ 8.11.4.

36. *Id.* (which states that "indirect effects of an attack may be one of the factors included when weighing anticipated incidental injury or death to protected persons").

37. Prosecutor v. Stanislav Galic, Case No. IT-98-29-T, Judgment, ¶ 58 (Int'l Crim. Trib. for the former Yugoslavia Dec. 5, 2003) (where the Trial Chamber held "[i]n determining whether an attack was proportionate, it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack").

38. John Markoff & Thom Shanker, *Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk*, NEW YORK TIMES (Aug. 1, 2009), http://www.nytimes.com/2009/08/02/us/politics/02cyber.html?_r=0.

ly mapping and monitoring the targeted computer or network, he will not be able to make a reasonable assessment of what effects are expected.

IV. FEASIBILITY

The legal standard of feasibility appears in several places in the "Precautions in Attack" section of API[39] and applies to most types of attacks.[40] In various provisions, a commander must do "everything feasible"[41] or "take all feasible precautions."[42] During the ratification process, there was great debate about the term "feasible" and what it meant.[43] A number of representatives to the negotiating convention made specific comments about the meaning "feasible" was to have when applied as a legal standard. John Redvers Freeland, the head of the United Kingdom delegation, through several sessions stated that the words "to the maximum extent feasible" related to what was "workable or practicable, taking into account all the circumstances at a given moment, and especially those which had a bearing on the success of military operations."[44] Similarly, S.H. Bloembergen, a delegate from the Netherlands, stated that "feasible" should be "interpreted as referring to that which was practicable or practically possible, taking into account all circumstances at the time."[45] As a result, "feasible" is generally understood to mean that which is "practicable or practically possible, taking into account all circumstances ruling at the time."[46]

---

39. API, *supra* note 15, arts. 57.2(a)(i)–(ii), 58.

40. *Id.*, art. 57.4; API COMMENTARY, *supra* note 16, at 704; TALLINN MANUAL, *supra* note 7, sec. 7.

41. API, *supra* note 15, art. 57.2(a)(i).

42. *Id.*, art. 57.2(a)(ii).

43. 14 Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts 199 (1978) [hereinafter Official Records].

44. 6 *id.* at 214; Jensen, *supra* note 19, at 1548.

45. 6 *id.* at 214; Jensen, *supra* note 19, at 1549.

46. Reservation Letter from Christopher Hulse, Ambassador from the United Kingdom to Switzerland, to the Swiss Government (Jan. 28, 1998), *available at* http://www.icrc.org/ihl.nsf/NORM/0A9E03F0F2EE757CC1256402003FB6D2?OpenDocument (listing the United Kingdom's reservations and declarations to Additional Protocol I, and explaining in paragraph (b) that "[t]he United Kingdom understands the term 'feasible' as used in the Protocol to mean that which is practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations"). *See also* UK MANUAL, *supra* note 16, ¶ 5.32; ICRC CIL STUDY, *supra* note 16, at 54.

A. "Practicable or Practically Possible"

During the API negotiations mentioned above, the national representatives were anxious to set a standard that would require diligence on the part of the commander, but would not be one with which it was beyond his capability to comply. The resulting language of practicality was the eventual resolution, which seems to be a workable standard in applying precautions in the attack.

The application of "feasibility" to cyber attacks seems ultimately tied to technology. As a commander contemplates a potential cyber attack, his "feasible precautions" should require him to sufficiently map the networks to determine the effects of the attack, particularly on civilians and civilian objects. This is much like the duty of constant care, but should carry a heightened specificity when planning a specific attack.

If in the process of preparing a cyber attack, the commander is unable to determine the extent of the attack's effects, he cannot launch an attack that would otherwise be considered indiscriminate. Or, if an attacker is unable to gather sufficient information as to the nature of a proposed target system, he should limit the attack to only those parts of the system for which he does have sufficient information to verify their status as lawful targets. In other words, the feasibility limitation should not be used as a justification for conducting an attack.

B. Circumstances Ruling at the Time

Without detracting from the duty of constant care previously discussed, the commander's duty to do what is feasible is limited by his circumstances. This limitation on commanders' liability stems from the post-World War II prosecution of German general Lothar Rendulic.[47] General Rendulic conducted a scorched-earth policy in Finnmark to slow what he thought were swiftly advancing Russian troops. In the end, the Russians were not coming as quickly as Rendulic had thought and the destruction proved to be unnecessary. However, the Military Tribunal determined that the legal standard was "consideration to all factors and existing possibilities" as they "appeared to the defendant at the time."[48]

---

47. *See* United States v. Wilhelm List and others, XI Trials of War Criminals Before the Nuernberg Military Tribunals Under Control Council Law No. 10, at 1295 (1950) [hereinafter Hostage Judgment]; *see also* Jensen, *supra* note 26, at 1181–83.

48. Hostage Judgment, *supra* note 47, at 1296.

This same standard should apply to the understanding of "feasibility" in cyber attacks. While commanders are required to do everything practicable, the responsibility is limited to the circumstances as the commander knows them at the time. For example, if a commander has used his best technology to map a network and exercises continuous monitoring in preparation for the attack, he has not violated the law if, during the course of the attack, the malware spreads unexpectedly to a civilian network that the commander did not know was linked to the military system.

V. PRECAUTIONS AGAINST THE EFFECTS OF ATTACKS

In addition to considering precautions when conducting attacks, nations have an obligation to take precautions against the potential effects of attacks.[49] Unlike the provisions discussed above that govern the conduct of attacks, this standard is not only a wartime standard. Rather, it is a standard that applies to nations during peacetime, in anticipation that armed conflict might arise in the future that would affect civilians and civilian objects.

Article 58 reads:

> The Parties to the conflict shall, to the maximum extent feasible:
>
> (a) Without prejudice to Article 49 of the Fourth Convention, endeavour to remove the civilian population, individual civilians and civilian objects under their control from the vicinity of military objectives;
> (b) Avoid locating military objectives within or near densely populated areas;
> (c) Take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations.[50]

This provision of the law is binding on nations only in international armed conflict, and is considered part of customary international law.[51] The

49. *See generally* TALLINN MANUAL, *supra* note 7, rule 59 (discussing precautions against the effects of attacks in relation to cyber operations).

50. API, *supra* note 15, art. 58.

51. ICRC CIL STUDY, *supra* note 16, at 68–69, 71, 74; NIAC MANUAL, *supra* note 16, ¶ 2.3.7; YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 145 (2d ed. 2010).

cyber aspects of Article 58 have been thoroughly discussed recently.[52] It is sufficient here to say that it establishes two layers of responsibility. Initially, a nation has the obligation to segregate its military objectives from civilians and civilian objects. Second, for those military objectives that it cannot segregate, the nation has a responsibility to protect the civilians and civilian objects from the anticipated effects of attacks.

Importantly, those who wrote this provision of API discussed in some detail the difficulty of accomplishing this standard. The inclusion of the caveat "to the maximum extent feasible" was the basis of much discussion and was purposely added in a way to apply to the entire provision, meaning that both the segregate and protect requirements are limited by the feasibility of any required actions.[53] This is also reflected by the ICRC in the *Commentary*, which states that "it is clear that precautions should not go beyond the point where the life of the population would become difficult or even impossible."[54]

One more important point is worth noting before discussing the obligations in detail. The title of Article 58 specifically refers to "attacks"; however, Article 58(c) refers to "operations," which cover a much broader spectrum of cyber activities. There is no doubt that the provisions discussed below, even those under the heading of "Protect," apply to precautions against potential cyber attacks, but the extent to which these provisions apply to operations is unclear, particularly for State parties to API. For nations like the United States who are not parties and are only bound by this article to the extent that it reflects customary international law, it seems clear that the customary aspect of this rule applies only to "attacks" and not all operations. The news is replete with examples of attacks on military objectives that impact civilian infrastructure and systems, and no States appear to have accepted the obligation to protect these targets.[55]

---

52. *See generally* Jensen, *supra* note 19.

53. Official Records, *supra* note 43, at 199.

54. API COMMENTARY, *supra* note 16, at 692.

55. *Security experts admit China stole secret fighter jet plans*, THE AUSTRALIAN, Mar. 12, 2012, World at 9, *available at* http://www.theaustralian.com.au/news/world/security-experts-admit-china-stole-secret-fighter-jet-plans/story-fnb64oi6-1226296400154; Press Release, Permanent Select Committee on Intelligence, Statement by Chairman Rogers on Senate Cybersecurity Legislation (Aug. 2, 2012), *available at* http://intelligence.house.gov/press-release/statement-chairman-rogers-senate-cybersecurity-legislation; Alexander Melnitzky, *Defending America Against Chinese Cyber Espionage Through the Use of Active Defenses*, 20 CARDOZO JOURNAL OF INTERNATIONAL AND COMPARATIVE LAW 537 (Winter 2012).

A. Segregate

It is clear that this rule was originally written with a very "geographic" focus that is hard to translate to the cyber domain. Segregating a military armaments storage facility is geographically easier than segregating digital military communications. In fact, estimates of the U.S. Department of Defense digital traffic that traverses civilian-owned and -operated infrastructure are between 90 and 98 percent.[56] There is certainly still a geographic aspect to the rule, even in the cyber domain, but there is also a virtual location aspect to the provision.

The distinction between the virtual and geographic natures of this rule in its application to cyber operations is exemplified by the difference between cyber infrastructure and digital communications. A nation can comply with the geographic nature of the requirement by positioning servers and other military cyber equipment away from civilian areas. Similarly, a nation could conceivably create a separate cyber infrastructure backbone upon which its military cyber communications would traverse, effectively segregating it from civilian infrastructure. This has obviously not been the practice of States to this point.

Rather, the ubiquitous nature of the cyber domain has made it almost impossible to segregate potential military objectives from civilian objects even in a geographic sense. Consider air traffic control centers and other major civilian transportation control centers, as well as power generation facilities. All of these serve both civilian and military purposes and are clearly cyber targets, but they are also virtually impossible to segregate. State practice in this area has at least demonstrated that nations have not found such segregation to be feasible.

In fact, many militaries seem to be moving in the exact opposite direction and co-locating an ever greater percentage of their cyber infrastructure with civilian infrastructure. A good example of this is the movement of military and government data to the "cloud."[57] While this move is heralded as providing great financial savings, it is unclear whether the legal obliga-

56. *See* McConnell, *supra* note 19.

57. CHIEF INFORMATION OFFICER, DEPARTMENT OF DEFENSE, CLOUD COMPUTING STRATEGY (2012), *available at* http:/www.defense.gov/news/DoDCloudComputing Strategy.pdf; John Keller, *U.S. Military Begins Moving Its Information Technology (IT) Infrastructure to Secure Cloud Computing*, MILITARY & AEROSPACE ELECTRONICS (July 29, 2012), http://www.militaryaerospace.com/articles/2012/07/dod-cloud-computing.html.

tion of segregation of military objectives was ever considered as part of the decision to use the cloud.

B. Protect

Given the difficulty of segregating military objectives from civilians and civilian objects in the cyber domain, the subsequent duty to protect civilians and civilian objects from the indirect effects of attacks on non-segregable military objectives becomes very important. The caveat of feasibility applies equally to this portion of the legal obligation, but the descriptive wording of "maximum extent" must also be allowed to have some meaning or the provision carries no legal weight at all.

1. "Dangers"

The requirement to protect does not encompass every potential cyber inconvenience or irritation. Rather, it applies only to "dangers" that might result from military operations. While this term is not defined in API, it seems reasonable to equate this standard to that used in the proportionality analysis discussed above, i.e., death or injury to civilians and damage to civilian objects.

Therefore, the protection obligation would not apply to cyber operations such as a denial of service attack that prevents access to a website or the altering of a website to change its appearance or connecting links. Instead, the obligation to protect should be understood to protect civilians and civilian objects from death or injury and destruction, such as shutting down air traffic control systems or power systems, which would result in serious effects on civilians.

2. "Under Their Control"

Another aspect of this rule that limits its general application is the use of the words "under their control." The plain reading of the obligation makes it clear that governments are not expected to protect all civilians and civilian objects from the effects of attacks, but only those which fall under the government's control.

As with the general rule, this particular provision was originally conceived territorially. In the drafting debates, the Canadian representative, Brigadier General Wolfe, argued to change the originally proposed lan-

guage of "authority" to "control" to make clear the de facto nature of the obligation.[58] The change was accepted and the obligation amended. In the cyber context, the de facto nature of the rule has significant impact. A government might claim that it does not have authority over most of the cyber infrastructure due to the various legal regimes that exist within the nation. However, under the de facto standard, if the party can dictate the operations of a civilian computer system, it is under the control of that party and the duty to segregate or protect applies.

3. Specific Measures

The ICRC *Commentary* to Article 58 suggests examples of specific measures that a nation could take to fulfill its obligations under the rule, including providing well-trained civil defense forces, systems for warnings of impending attacks, and responsive fire and emergency services.[59] Analogizing these suggestions to the cyber world would suggest actions such as providing or requiring protective software products, monitoring networks and systems and providing warnings of impending or ongoing attacks, and providing technical assistance to repair networks or reroute them to alternative systems that continue to maintain functionality.

The U.S. government has already started to take some of these actions, though the extent to which it is taking them as a result of its legal obligation is unclear. For example, the United States has recently started the Defense Industrial Base Pilot Program, which is now expanding.[60] Under the program, specific industries providing defense services that make them legitimate targets in an armed conflict must meet certain cybersecurity requirements in order to do business with the government. Additionally, they receive some cyber assistance as a result of their membership in the program.

Additionally, the U.S. government recently stated that it will warn industries when they appear to be the target of an attack in an attempt to put

58. 14 Official Records, s*upra* note 43, at 198–99 (where it states, "[T]he use of the word 'control' would impose obligations on the parties which would not necessarily be implied by the use of the word 'authority.' It referred to the de facto as opposed to the de jure situation.").

59. API COMMENTARY, *supra* note 16, at 694–95; *see also* ICRC CIL STUDY, *supra* note 16, at 70.

60. News Release, U.S. Department of Defense, DOD Announces the Expansion of Defense Industrial Base (DIB) Voluntary Cybersecurity Information Sharing Activities (May 11, 2012), http://www.defense.gov/releases/release.aspx?releaseid=15266.

them on notice so they can increase their security posture.[61] Interestingly, the cyber giant Google has also recently announced that it will provide warnings to clients that appear to be the target of "State" hacking operations.[62] While Google certainly does not have any legal obligation under Article 58 to do so, it is interesting to note the sense that there is a need for such warnings.

Finally, the recent coordination between Google and the National Security Agency after the former was the victim of attacks from the Chinese government[63] may foreshadow an emerging cyber era where the government not only provides warning information, but then works closely to remediate and potentially retaliate for State-sponsored cyber activities that affect key civilian industries.

As a closing point to this part, it is important to note that a nation's inability or failure to fulfill its obligations under Article 58 does not affect an adversary's legal ability to conduct cyber attacks, so long as those attacks comply with the applicable rules of the LOAC.

VI. CONCLUSION

Cyber warfare is governed by the LOAC, and the LOAC does a generally good job of regulating cyber operations. In most cases, the existing law provides a clear paradigm to govern cyber activities; however, there are several areas where governments and military operators might question how to apply the LOAC to a specific cyber operation. This article has highlighted a few areas where additional clarity would be useful, such as in the cases of the definition of attack, the details of applying constant care, and

---

61. Lolita C. Baldor, *Pentagon Warns Public About Cyber Attacks by China*, BOSTON.COM (Aug. 20, 2010), http://www.boston.com/news/nation/washington/articles/2010/08/20/pentagon_warns_public_about_cyber_attacks_by_china/; Michael Finnegan, *US Government Warns over Gas Pipeline Cyberattacks*, TECHEYE.NET (May 9, 2012, 3:14 PM), http://news.techeye.net/security/us-government-warns-over-gas-pipeline-cyberattacks.

62. Hayley Tsukayama & Ellen Nakashima, *Google to alert users about state-sponsored cyberattacks*, WASHINGTON POST, June 6, 2012, at A5, *available at* http://www.washingtonpost.com/business/economy/google-to-alert-users-about-state-sponsored-attacks/2012/06/05/gJQA.zS8GV_story.html.

63. Ellen Nakashima, *Google to enlist NSA to help it ward off cyberattacks*, WASHINGTON POST, Feb. 4, 2010, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/03/AR2010020304057.html; *see also* Stephanie A. DeVos, Note, *The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed*, 21 FORDHAM INTELLECTUAL PROPERTY, MEDIA AND ENTERTAINMENT LAW JOURNAL 173 (2010).

the required precautions against the effects of attacks. As the discussion on these issues increases, particularly spurred by the *Tallinn Manual*, and as State actions in cyberspace inevitably increase, State practice will provide nuance to the application of the LOAC that will allow clearer definition on the use of cyber operations in armed conflict.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Computer Network Operations and U.S. Domestic Law: An Overview

Robert M. Chesney

89 INT'L L. STUD. 218 (2013)

Volume 89 2013

Computer Network Operations and U.S. Domestic Law: An Overview

Robert M. Chesney[*]

I. INTRODUCTION

Computer network operations (CNOs) famously give rise to a number of international law complications, and scholars have duly taken note.[1] But

* Charles I. Francis Professor in Law, University of Texas School of Law.

1. This was, of course, the primary subject of the conference of which this article was a part. *See* U.S. Naval War College International Law Department, 2012 ILD Conference: "Cyber War and International Law," http://www.usnwc.edu/ILDJune2012. It was also the subject of the International Law Department's 1999 conference, "Computer Network Attack and International Law." The papers resulting from that conference may be found in COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (Vol. 76, U.S. Naval War College International Law Studies). For a sampling of the considerable literature focused on the international law questions raised by CNOs, see Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIFORNIA LAW REVIEW 817 (2012); Hannah Lobel, *Note: Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict,* 47 TEXAS INTERNATIONAL LAW JOURNAL 617 (2012); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421 (2011); Michael N. Schmitt, *Cyber Operations and the Jus ad Bellum Revisited*, 56 VILLANOVA LAW REVIEW 569 (2011); Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEXAS LAW REVIEW 1533 (2010); Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 63 (2010). *See also* TALLINN MANUAL ON

CNOs also raise important questions under the heading of U.S. domestic law, particularly when the government does not intend for its sponsoring role to be apparent or acknowledged. Those domestic issues have received comparatively little attention.[2]

This article introduces readers to four of the most important domestic law questions raised by CNOs, drawing on my prior work exploring the disruptive impact of organizational and technological change on the legal architecture of national security activities.[3] First, must Congress be notified of a given CNO and, if so, which committee should receive that notice? Second, must the CNO in question be authorized by the President himself, or can authority be moved down the chain to other officials—or perhaps even automated? Third, what is the affirmative source of domestic law authority for the executive branch to conduct various types of CNO? Fourth, and finally, does categorizing a CNO as covert action subject to Title 50 of the U.S. Code (U.S.C) carry with it a green light (from a domestic law perspective) to violate international law?

II. MUST CNOS BE REPORTED TO CONGRESS?

The issue with respect to congressional oversight is whether the executive branch must give notice of a given CNO (or programmatic series of CNOs) to (i) the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence (collectively, the Intelligence Committees), (ii) to the Senate Armed Services Committee and the House Armed Services Committee (collectively, the Armed Services Committees), (iii) to both pairs or (iv) to none of the above.

This general topic is familiar to American national security law practitioners from the context of covert action. Pursuant to § 503 of the Nation-

---

THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

2. Notable exceptions that address domestic issues at least in part include Aaron P. Brecher, *Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations,* 111 MICHIGAN LAW REVIEW 423 (2012); Robert D. Williams, *(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action*, 79 GEORGE WASHINGTON LAW REVIEW 1162 (2011); Steven G. Bradbury, *The Developing Legal Framework for Defensive and Offensive Cyber Operations*, 2 HARVARD NATIONAL SECURITY JOURNAL 591 (2011); Paul A. Walker, *Traditional Military Activities in Cyberspace: Preparing for "Netwar,"* 22 FLORIDA JOURNAL OF INTERNATIONAL LAW 333 (2010).

3. *See* Robert M. Chesney, *Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate*, 5 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 539 (2012).

al Security Act, the executive branch must provide notification of a "covert action" to the Intelligence Committees (though notification can be limited in "extraordinary circumstances" to the "Gang of Eight"—i.e., the chairs and ranking members of both committees, as well as the Speaker and Minority Leader in the House and the Majority and Minority Leaders in the Senate).[4] "Covert action," in turn, is defined by statute to mean "an activity . . . of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the . . . government will not be apparent or acknowledged publicly . . . ."[5]

So far so good. It is easy to understand how a CNO conducted for purposes of sabotage, for example, implicates that definition at first blush. But the statute goes on to carve out a series of exceptions to the covert action definition,[6] two of which make it relatively difficult to determine—particularly in advance—whether a given CNO triggers the covert action oversight framework.

First, an otherwise-qualifying activity does not count as "covert action" if its "primary purpose . . . is to acquire intelligence . . . ."[7] A CNO certainly might be designed primarily to acquire intelligence, whether through keystroke logging, network mapping, microphone or camera control, or data copying.[8] But this turns out to be irrelevant insofar as congressional notification is concerned, because the National Security Act separately provides that significant intelligence activities—including activities to collect intelligence—also must be reported to the Intelligence Committees.[9] Categorizing a CNO as intelligence-gathering rather than covert action thus does nothing to alter the obligation to keep Congress informed.

The second relevant exception to the definition of covert action is different. It encompasses "traditional . . . military activities" (often referred to as TMA) and "routine support" thereto.[10] When it applies the executive branch has no obligation to keep the Intelligence Committees informed of the activities in question, period.

---

4. 50 U.S.C. § 413b(b), (c) (2006).

5. *Id.*, § 413(e).

6. *Id.*, § 413(e)(1–4).

7. *Id.*, § 413(e)(1).

8. *See, e.g.,* Kim Zetter, *State-Sponsored Malware "Flame" Has Smaller, More Devious Cousin*, WIRED (Oct. 15, 2012, 8:00 AM), http://www.wired.com/threatlevel/2012/10/miniflame-espionage-tool/

9. 50 U.S.C. §§ 413, 413a (2006).

10. *Id.*, § 413(e)(2).

Consider first the scope of the TMA exception. The text of the statute does not define TMA. This naturally tempts some to assume that the key to identifying activity as TMA involves some form of comparison to past practices particularly associated with the military. The word "traditional" in TMA, after all, suggests precisely this comparison. If that were indeed the correct reading, substantial debates would then arise in light of the relative novelty of CNOs. In order to categorize a CNO as TMA, one would first have to establish that the TMA standard could be satisfied via analogy rather than requiring a literal precedent showing the military previously engaged in that exact type of operation. If that bridge were crossed, moreover, one would then have to show that the CNO in question does in fact track the relevant contours of some past, non-cyber military operations. The history-based interpretation of TMA, in short, invites no small amount of disagreement and instability. But it is far from clear that the history-based interpretation of TMA is correct in the first place.

The legislative history of the TMA exception is long and dense, and I have set it forth in its full complexity elsewhere.[11] For present purposes, it suffices to observe that Congress and the administration of George H.W. Bush negotiated this question extensively, and ultimately compromised by adopting a relatively objective definition of TMA.[12] Two conditions had to be met, no more and no less. First, the activity had to be commanded and executed by military personnel. Second, the activity had to take place in a context in which *overt* hostilities either were under way already or at least were "anticipated" in the specific sense that the National Command Authorities had authorized "operational planning for hostilities."[13] Historical comparisons simply did not enter into the picture, on this view.

This understanding—*if* accepted by all sides engaged in an internal debate over the applicability of the TMA exception in a given case—should prove relatively easy to map onto CNOs in some contexts. Most obviously, any CNO linked to overt combat operations, such as those currently under way in Afghanistan, should qualify without controversy (so long as commanded and executed by military personnel). Similarly, an operation like Stuxnet—involving a potential adversary regarding which it is quite possi-

11. *See* Chesney, *supra* note 3, at 592–601. *See also* Walker, *supra* note 2.

12. *See* Walker, *supra* note 2, at 340 (citing S. REP. NO. 102-85, at 46 (1991); H.R. CONF. REP. 102-166 (1991)).

13. S. REP. NO. 102-85, at 46 (1991).

ble if not probable that operational planning has been authorized—likewise would qualify so long as commanded and executed by military personnel.[14]

Why then might there still be controversy with respect to TMA's scope? First, it is not obvious that the objective, negotiated definition just discussed is, in fact, widely appreciated within the government, let alone widely accepted as controlling. It is memorialized only in the legislative history rather than the actual text of the statute, after all, and it does not follow intuitively from the words "*traditional* military activity." Second, even if one accepts the objective test, there remains significant room for disagreement regarding its actual application, particularly thanks to ongoing uncertainty over the organizational, geographic and temporal scope of hostilities relating to al Qaeda and the conflict once called the "war on terror."

And what of "routine support" to TMA? This too was the subject of considerable attention during the drafting of the covert action definition.[15] Rather than adopt specific criteria to explain the boundaries of the routine support concept, Congress in the legislative history provided an illustrative set of examples. Unacknowledged logistical support for a potential military operation would count, for example, whereas recruiting foreign personnel or engaging in propaganda would not. The difference, according to the legislative history, was that the latter were riskier activities for the United States, hence less appropriate for exemption from the oversight system. That risk-oriented distinction can be brought to bear on the question whether a given CNO constitutes routine support to TMA, but one should expect there to be many circumstances in which reasonable minds can disagree as to the outcome; the nature of this criterion is simply too subjective, whether we are speaking of CNOs or non-cyber activities.

In any event, let us assume now that a given CNO qualifies as TMA or routine support thereto. Might there still be an obligation to report it to Congress?

---

14. This helps us make sense of what David Sanger reports with respect to Stuxnet:

> At the insistence of Defense Secretary Robert Gates, the program had been shifted over from military command to the intelligence community. That meant that President Obama had to review and renew a set of presidential findings that would allow the United States to attack the nuclear infrastructure of a country with which we were not at war.

DAVID E. SANGER, CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER 200–201 (2012). A presidential "finding," as I explain below in Part II, becomes necessary only upon a determination that the activity is a covert action rather than TMA.

15. *See* S. REP. NO. 101-358, at 54 (1990).

On one hand, 10 U.S.C. § 119 does specify that new special access programs may not be initiated by the Department of Defense without notification to the Armed Services Committees.[16] This might encompass some CNOs. But it would not necessarily encompass all of them, and in any event would not require the sort of detailed, high-granularity exchange of information that can arise with covert action oversight. Of course, relatively detailed reporting *might* occur even without an explicit statutory obligation; the Armed Services Committees and their staffs obviously have significant leverage, and as a practical matter can demand no small amount of transparency if the leadership so desires. At the end of the day, however, the fact remains that categorization as TMA or routine support to TMA removes the statutory requirement of relatively granular reporting to Congress.

III. MUST CNOS BE APPROVED BY THE PRESIDENT?

Whether a given CNO constitutes covert action has implications beyond notification to Congress. The National Security Act not only requires reporting of covert action to the Intelligence Committees, but also specifies that such activity must be authorized in a written "finding" signed by the President. This requirement of a presidential finding serves to constrain the executive branch in at least a couple of ways. First, and most obviously, it precludes the President from later denying knowledge of what might turn out to be a controversial action, thus giving rise to top-down pressure to screen out risky proposals (for better or worse). Second, and relatedly, the process of generating a presidential finding generally involves input from multiple departments, some of whom may have distinct or competing equities at stake and hence incentive to argue for modification or rejection of the proposal.

Categorizing a CNO as covert action automatically brings these constraints to bear. But as I explained in Part I there are circumstances in which a CNO might more accurately be characterized as either TMA or intelligence collection. What then?

If a CNO constitutes TMA, the question whether a statute requires approval from a particular official becomes complicated. At first blush, there appears to be no such obligation. And that is indeed the end of the analysis for those who reject the negotiated definition of TMA (described above in

16. 10 U.S.C. § 119 (2006).

Part I). Those who accept the negotiated definition, however, must go on to ask one further question. Recall that the negotiated definition of TMA distinguishes between activities conducted in the context of ongoing hostilities and those conducted in relation to anticipated hostilities for which operational planning has been authorized. Under the ongoing-hostilities track, there is no requirement that a particular official approve the activity in question in order for it to qualify as TMA. But under the anticipated-hostilities track, the answer is different. The negotiated definition specifies that the activity must be approved by the National Command Authorities—i.e., the President or Secretary of Defense—in order for it to qualify as TMA in such circumstances.[17]

What if the CNO in question instead is best understood as intelligence collection rather than covert action or TMA? I noted in Part I that classification of a CNO as collection did not alter the obligation to report the activity to the Intelligence Committees. The intelligence-collection/covert action distinction does matter, in contrast, with respect to the question of statutorily required authorization. Whereas a presidential finding is required for covert action, there is no parallel or comparable statutory requirement for intelligence-collection operations.

Unfortunately, it is not necessarily easy to apply the intelligence-collection/covert action distinction, particularly in the CNO setting. The code in question may involve a complex suite of tools including not just capacities for collection, but also capacities to disrupt or modify the operation of an infiltrated system or server (as appears to have been the case with the so-called Stuxnet CNO directed at Iran).[18] The "primary purpose" criterion built into the statutory language anticipates such dual-use problems in the abstract, calling for what amounts to a center-of-gravity test. That inquiry is both subjective and dependent upon timing, however. What might seem to be the code's primary purpose might appear to be collection at one point in time, and disruption at some later point (e.g., after the previously latent destructive capacity of the code has been employed). The National Security Act, alas, does not provide guidance regarding which moment is the correct one on which to focus or whether the inquiry should be conducted repeatedly over time.

Of course, a statute is not the only means by which a requirement of high-level approval for CNOs could be imposed. The President himself

17. *See supra* note 13 and accompanying text.

18. *See* SANGER, *supra* note 14, at 190–206.

can issue such a mandate, after all, and it does appear from the public record that something along these lines has occurred. A series of media accounts in recent years tell the tale of long-running interagency disputes as the Pentagon attempts to craft rules of engagement determining when CNOs might be conducted in contexts that could have adverse effects on systems physically located outside the United States, with at least some circumstances marked as off-limits without presidential approval.[19]

IV. MUST CNOS BE SUPPORTED BY CONGRESSIONAL AUTHORIZATION?

CNOs come in many shapes and sizes, some of which are uninteresting from a separation-of-powers perspective. Those that are best analogized to intelligence gathering, for example, should be relatively easy to explain with reference to the same combination of Article II constitutional authorities and statutes that justify such activity in non-cyber settings.[20] Where a CNO instead constitutes TMA or covert action, however, difficult (or at least more interesting) questions can arise.

As a threshold matter, it is worth noting that separation-of-powers concerns drop out to the extent that a given CNO falls within the scope of a statutory authorization for use of military force, such as the still-operative Authorization for the Use of Military Force (AUMF) enacted after 9/11.[21] That AUMF famously provides that the President may use "all necessary and appropriate force" against those entities or individuals he determines were responsible for the 9/11 attacks, as well as entities or individuals harboring them. In some instances involving CNOs, it will be fairly obvious that the AUMF applies. If the Afghan Taliban have a recruiting website hosted on a server in Afghanistan, for example, a U.S. Cyber Command

19. *See* Ellen Nakashima, *Pentagon Seeks More Powers for Cyberdefense*, WASHINGTON POST, Aug. 10, 2012, at A1; Lolita Baldor, *Pentagon Still Grappling with Rules of Cyberwar*, ASSOCIATED PRESS, July 25, 2012, *available at* http://www.foxnews.com/us/2012/07/25/pentagon-still-grappling-with-rules-cyberwar/; Ellen Nakashima, *A Cyberspy Is Halted, but Not a Debate,* WASHINGTON POST, Dec. 9, 2011, at A1; ERIC SCHMITT & THOM SHANKER, COUNTERSTRIKE: THE UNTOLD STORY OF AMERICA'S SECRET CAMPAIGN AGAINST AL QAEDA 135–36, 145–46 (2011).

20. *See* Williams, *supra* note 2, at 1167 ("Authority for foreign intelligence collection by the United States Government is grounded in the 'firm foundation' of the Constitution, the National Security Act of 1947 . . . and the Central Intelligence Act of 1949, as well as the many congressional appropriations for intelligence activities.").

21. *See* Pub. L. No. 107-40, 115 Stat. 224 (2001) (Sept. 18, 2001). For a detailed and insightful discussion of this topic, see Brecher, *supra* note 2.

operation to disrupt that website rather plainly would fall within the AUMF's scope. If that server is instead located in Dubai or Germany, however, and if the organization in question is not al Qaeda or the Afghan Taliban but instead some meaningfully-distinct group, things begin to look less clear. Prompted by controversy surrounding detention and drone strikes, there has for many years been a debate about the AUMF's precise boundaries in terms of its geographic and organizational scope, and that debate is growing more serious over time as the center of gravity for AUMF-related operations moves away from Afghanistan, the Afghan Taliban, and the core al Qaeda leadership.[22] CNOs may have implicated these questions in the past; they certainly will do so in the future.

If a given CNO does *not* plausibly fall within the scope of the AUMF, what then? Many non-AUMF CNOs are best categorized as intelligence-collection operations, as noted above, and those typically do not raise significant separation-of-powers concerns. Other non-AUMF CNOs instead constitute covert action or TMA, yet should not be controversial from a separation-of-powers perspective either, because they may be supported by other forms of statutory authorization or by plausible claims that they are within the scope of the President's Article II authorities. A CNO conducted by the Central Intelligence Agency (CIA) as covert action, for example, may rest on the same statutory foundation as any other covert action conducted by the agency: i.e., the National Security Act's "fifth function" as fleshed out over time by executive branch practice, congressional acquiescence in that practice and subsequently enacted oversight legislation.[23] And at least some instances of non-AUMF CNOs constituting either covert action or TMA (particularly those that are distant in their nature or effects from the use of kinetic force) might be relatively easy to justify as exercises of the constitutional authority of the President to conduct foreign affairs or to command the armed forces.[24]

Is the latter still true for a CNO with significant kinetic effects, such as Stuxnet?[25] In 2011, the Obama administration contended that its sustained,

---

22. *See* Robert M. Chesney, *Beyond the Battlefield, Beyond al Qaeda: The Destabilizing Legal Architecture of Counterterrorism*, MICHIGAN LAW REVIEW (forthcoming 2013).

23. *See, e.g.,* William C. Banks & Peter Raven-Hansen, *Targeted Killing and Assassination: The U.S. Legal Framework*, 37 UNIVERSITY OF RICHMOND LAW REVIEW 667, 698 (2003).

24. *Cf.* Robert F. Turner, *Coercive Court Action and the Law,* 20 YALE JOURNAL OF INTERNATIONAL LAW 427, 442–45 (1995) (reviewing W. MICHAEL REISMAN & JAMES E. BAKER, REGULATING COVERT ACTION: PRACTICES, CONTEXTS, AND POLICIES OF COVERT COERCION ABROAD IN INTERNATIONAL AND AMERICAN LAW (1992)).

25. *See* SANGER, *supra* note 14.

overt use of airpower in Libya (including both comprehensive logistical support to combat sorties carried out by NATO and other allies, and periodic airstrikes using U.S. manned and unmanned aircraft) fell within the President's constitutional authority to act in foreign affairs in pursuit of significant national interests, and that this did not infringe congressional prerogatives over the resort to war in light of the limited nature of the force involved, the limited purposes for which it was being used, and the fact that the situation did not entail a significant risk of harm to U.S. personnel.[26] Few if any CNOs would run afoul of that narrow understanding of the congressional role. That said, the Obama administration's theory of authority vis-à-vis Libya has been met with sharp criticism, and reliance exclusively upon it might be unnecessarily risky.[27] If the circumstances warrant the argument,[28] it would be wise instead (or at least in addition) to invoke the President's constitutional duty to use force in self-defense, a duty which if otherwise implicated can surely encompass CNOs.[29]

---

26. *See* Office of Legal Counsel, *Authority to Use Force in Libya*, 35 Op. O.L.C. (Apr. 1, 2011), *available at* http://www.justice.gov/olc/2011/authority-military-use-in-libya.pdf.

27. *See, e.g.,* Michael D. Ramsey, *Meet the New Boss: Continuity in Presidential War Powers?*, 35 HARVARD JOURNAL OF LAW AND PUBLIC POLICY 863, 864 (2012).

28. The precise boundaries of self-defense authority are famously difficult to define. Much of the literature on this subject arises in the international law setting. *See, e.g.,* Matthew C. Waxman, *The Use of Force Against States That Might Have Weapons of Mass Destruction*, 31 MICHIGAN JOURNAL OF INTERNATIONAL LAW 1 (2009). To at least some extent, however, the insights of the international law debate can be mapped onto the parallel separation-of-powers questions associated with the President's self-defense authority. In practical terms relating to CNOs, the hardest questions may arise when the government acts in an anticipatory rather than reactive setting. *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework,* 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885, 932–33 (1999). *See also* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARVARD JOURNAL OF LAW & TECHNOLOGY 415, 526–28 (2012); David E. Graham, *Cyber Threats and the Law of War*, 4 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 87, 90 (2010).

29. David Sanger's account of the internal debates of the Obama administration in relation to the use of force in Libya in 2011 raises an interesting question. According to his account, U.S. officials at one point considered conducting a CNO that might disable Libya's air defense network, prior to overt military intervention. *See* SANGER, *supra* note 14, at 344. The proposal came to naught in the face of technical difficulties, but along the way it apparently generated a legal dispute "about whether the President had the authority . . . to order a cyberattack as part of a broader military operation without first consulting Congress." *Id.* It is unclear how resort to a CNO could possibly have raised different separation-of-powers concerns than the overt, kinetic measures the Obama administration was contemplating, let alone concerns with more bite. It may be that the actual concern in this instance had more to do with fear of exposure of U.S. CNO capacities that might follow

Against this backdrop, one final question arises: For the subset of cases in which congressional authorization at least arguably is necessary, has Congress already provided such authorization separate and apart from the AUMF? This question draws our attention to § 954 of the National Defense Authorization Act for Fiscal Year 2012. That statute provides as follows:

> Congress affirms that the Department of Defense has the capability, and upon direction by the President may conduct offensive operations in cyberspace to defend our Nation, Allies and interests, subject to—
>
> (1) the policy principles and legal regimes that the Department follows for kinetic capabilities, including the law of armed conflict; and
> (2) the War Powers Resolution (50 U.S.C. 1541 et seq.).

The interesting question here is whether § 954 should be read to authorize CNOs in circumstances beyond what would be covered in any event either by the AUMF or by a plausible claim of inherent presidential authority, or whether instead § 954 merely confirms existing authority for clarity's sake (and perhaps also to dispel doubt that such existing authority requires compliance with the War Powers Resolution and various other regulatory regimes that would govern Department of Defense kinetic operations). Section 954 is clearly superfluous as an authorizing mechanism insofar as it contemplates CNOs in circumstances genuinely involving national self-defense. Whether the same can be said for the statute's explicit reference to "offensive" CNOs undertaken in the defense of "Allies and interests," however, is much less clear.

On its face, this language might be taken as a standing authorization to engage in CNOs for a rather wide range of purposes beyond those for which it is quite apparent authority already exists. But did Congress actually intend that result? There is reason to believe it did not, though the matter is far from conclusive.

The original version of this section—§ 962 in the House bill—simply stated that the military had authority to engage in CNOs on a clandestine basis when acting under color of the AUMF or "to defend against a cyber

---

from disclosure to Congress (under the War Powers Resolution (WPR)) that the United States had engaged in such an operation. Or it may simply be that participants in this debate took the view that a CNO of this kind would amount to the introduction of U.S. forces into hostilities, triggering the consultation language in section 3 of the WPR.

attack against an asset of the Department of Defense."[30] That language would have done little work other than helping to clarify the TMA/covert action distinction as applied to CNOs. Later, during the conference reconciliation process, that text was replaced by the language that became § 954—language that does not obviously speak to the TMA/covert action question. Despite this, the explanation for § 954 published by the conference committee focused on precisely that question:

> The conferees recognize that because of the evolving nature of cyber warfare, there is a lack of historical precedent for what constitutes *traditional military activities* in relation to cyber operations and that it is necessary to affirm that such operations may be conducted pursuant to the same policy, principles, and legal regimes that pertain to kinetic capabilities.[31]

Of course, the conference committee report also proceeded to address a separate point:

> The conferees also recognize that in certain instances, the most effective way to deal with threats and protect U.S. and coalition forces is to undertake offensive military cyber activities, including where the role of the United States Government is not apparent or to be acknowledged. The conferees stress that, as with any use of force, the War Powers Resolution may apply.[32]

Seen in this light, § 954's reference to "offensive" CNOs might best be understood to use "offensive" in the tactical sense of taking the initiative to attack the enemy in a particular instance, as distinct from the larger constitutional sense in which one might ask whether the U.S. government is initiating hostilities or instead acting overall in a defensive capacity. From this perspective, it is possible to undertake offensive operations while still under a larger defense rubric, and if that is indeed what § 954 is referring to then there is much less basis for construing the statute as a blank check to conduct CNOs in otherwise inappropriate circumstances.

---

30. National Defense Authorization Act for Fiscal Year 2012, H.R. 1540, 112th Cong. § 962 (2011).

31. Explanation of Funding Summary 146 (emphasis added), http://democrats.rules.house.gov/112/text/112_hr1540mgrs_txt.pdf(last visited Nov. 10, 2012).

32. *Id.*

V. MUST CNOS COMPLY WITH INTERNATIONAL LAW?

CNOs raise an array of international law issues, including questions of compliance with the law of armed conflict and international law protection for the sovereignty of States. Strictly speaking, such questions are beyond the scope of this article, as I am focused here exclusively on questions of domestic law.[33] There is, however, an important domestic law question lurking in the background when the subject of CNOs and international law arises: Does the statutory authority to conduct covert action under Title 50 entail standing, domestic law authorization for the executive branch to place the United States in violation of otherwise-applicable international law?

I previously addressed this question in some detail in the midst of a much-longer exploration of the so-called Title 10/Title 50 debate.[34] Nothing in Title 50, I observed then, explicitly authorized operations in violation of international law, nor did the legislative history of the covert action provisions of Title 50 suggest that Congress intended to confer a standing authorization to act contrary to international law rules so long as the government acted covertly.[35] There is, though, an additional argument I did not previously address.

The argument arises out of a conspicuous omission in § 503 of the National Security Act (50 U.S.C. § 413b(a)). Section 503 specifies that a presidential finding authorizing covert action may not call for conduct that would violate the Constitution or any federal statute. It says nothing of the kind, in contrast, about compliance with international law.[36] Did Congress intend thereby to authorize covert action in violation of international law, albeit without saying so explicitly?

It is possible that the executive branch reads Title 50 in this manner, yet it is far from certain that it does so. The most recent and detailed glimpse into the CIA's own perspective on its legal compliance obligations is a speech delivered at Harvard Law School in April 2012 by the CIA's General Counsel, Stephen W. Preston. In it, Preston provided an overview of how his office works through questions of domestic and international

33. *See, e.g.,* TALLINN MANUAL, *supra* note 1.
34. *See* Chesney, *supra* note 3, at 617–28.
35. *See id.*
36. *See* 50 U.S.C. § 413b(a)(5) (2006).

law compliance.[37] With respect to domestic law, Preston was clear about the CIA's compliance obligations: "[A]ll steps taken must comply with applicable prohibitions and limitations in the U.S. Constitution, federal statutes, executive orders and other presidential directives, and Agency regulations."[38] He separately observed that "international law principles may be applicable as well," later elaborating that if the CIA were to conduct operations involving the use of lethal force it "would implement its authorities in a manner consistent with the four basic principles in the law of armed conflict governing the use of force . . . ."[39] Some observers construed this language as indirect acknowledgment that the CIA does not actually think itself bound by international law, even if it does choose to comply with "principles" derived therefrom.[40] Notably, in this regard, the speech did include a pointed quotation of § 503, describing it as a "crucial provision" that "would be strictly applied in carrying out our hypothetical program."[41]

It is difficult to say whether this was a veiled acknowledgment that § 503 is understood within the CIA as permitting the President to direct the CIA to engage in conduct that might violate international law, or if instead it merely reflected a disposition to speak more directly about domestic law as the primary focus of legal review in such cases. The question does seem to matter in practice for CNOs, though, in light of the genuine prospect of undesired third-country (or at least third-party) effects. As one anonymous U.S. government official put the point recently: "Operations in the cyberworld can't be likened to Yorktown, Iwo Jima or the Inchon landing . . . . Defining the battlefield too broadly could lead to undesired consequences, so you have to manage the potential risks. Getting to the enemy could mean touching friends along the way.[42]"

More specifically, "getting to the enemy" with a CNO could mean disrupting the operation of a system or server that is physically located in the territory of a State that is not an enemy and that might not have consented

37. Stephen W. Preston, *CIA and the Rule of Law*, 6 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 1 (2012).

38. *Id.* at 3.

39. *Id.* at 3, 7.

40. *See, e.g.,* Deborah Pearlstein, *CIA General Counsel Speech on Hypothetical Uses of Force*, OPINIO JURIS (Apr. 11, 2012), http://opiniojuris.org/2012/04/11/cia-general-counsel-speech-on-hypothetical-uses-of-force/.

41. Preston, *supra* note 37, at 6.

42. Ellen Nakashima, *Pentagon's Cyber Command Seeks Authority to Expand Its Battlefield*, WASHINGTON POST (Nov. 6, 2010, 12:41 AM), http://www.washingtonpost.com/wp-dyn/content/article/2010/11/05/ar2010110507304.html.

to the intrusion, with damaging collateral consequences for any number of entities around the world who happen also to rely on those systems or servers. In addition to posing a policy dilemma, this fact pattern also raises international law questions—and hence collateral questions regarding international law compliance obligations when acting under the covert action rubric. The *Washington Post* reports that a dispute arising out of such concerns was put to the Justice Department's Office of Legal Counsel in 2010, resulting in a draft opinion to the effect that "[o]perations outside a war zone would require the permission of countries whose servers or networks might be implicated."[43] It was not clear, alas, whether the draft opinion specifically addressed the covert action question described above.[44]

VI. CONCLUSION

From a domestic law perspective, CNOs present a host of interesting and difficult questions. By and large they are the same questions that surround other forms of government activity in which the government's role might not be apparent or acknowledged. This overlap does not mean there are clear answers to the questions, however. In important respects, the law remains underdeveloped, and in any event the particular characteristics of CNOs at times may make these frameworks particularly difficult to apply.

43. *See id.*

44. It is important to bear in mind that there may be *other* reasons why the CIA, for example, might enjoy greater discretion than the military to conduct certain operations in certain locations. Most obviously, this will be the case where the military acts pursuant to an execute order that contains relatively strict constraints relating to which activities can be conducted in which locations, while the CIA acts pursuant to a covert action finding with broader parameters.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Classification of Cyber Conflict

Michael N. Schmitt

89 INT'L L. STUD. 233 (2013)

Volume 89 2013

Classification of Cyber Conflict

Michael N. Schmitt[*]

I. INTRODUCTION

Few international humanitarian law topics are proving as problematic in modern warfare as "classification of conflict," that is, the identification of the type of conflict to which particular hostilities amount as a matter of law.[1] Classifying the conflict in question is always the first step in any international humanitarian law analysis, for the nature of the conflict determines the applicable legal regime. Accordingly, classification is a subject of seminal importance.

The current difficulties derive from the advent of hostilities over the past two decades that do not neatly fit the traditional bifurcation of conflict

---

* Chairman, International Law Department, U.S. Naval War College. A previous version of this paper was published in 17 JOURNAL OF CONFLICT AND SECURITY LAW 245 (2012). The opinions shared in this paper are those of the author and do not necessarily reflect the views and opinions of the U.S. Naval War College, the Dept. of the Navy or Dept. of Defense.

1. For a comprehensive survey of the subject, including case studies, see INTERNATIONAL LAW AND THE CLASSIFICATION OF CONFLICT (Elizabeth Wilmshurst ed., 2011). The work is the culmination of a two-year Chatham House-sponsored project involving a group of international experts. This article has benefitted from participation in that process and the author is grateful to his colleagues for their insights.

into either State-on-State or purely internal. For instance, the International Criminal Tribunal for the former Yugoslavia (ICTY) struggled with criteria for internationalization of non-international conflict in its first case, *Tadić*.[2] Less than a decade later, transnational terrorism refocused attention on classification issues. Was such terrorism international in character because it transcended borders or non-international because it did not involve the forces of one State engaging in hostilities against those of another (or was it even armed conflict at all)?[3] More recently, external recognition of the National Transitional Council as the legitimate government of Libya raised the question of whether such recognition "de-internationalized" the conflict between the States that were fighting on the side of the rebels and Qaddafi's forces.[4]

In the future, cyber warfare will further complicate classification. Cyber operations have the potential for producing vast societal and economic disruption without causing the physical damage typically associated with armed conflict. They are also inherently transborder, thereby frustrating any approach to classification based on geographical factors. Moreover, massive attacks can be launched by a single individual or by a group that is organized entirely on-line. This is in sharp contrast to traditional warfare, which depends on either the involvement of a State's armed forces or that of a group capable of mounting typical military operations.

---

2. Prosecutor v. Tadić; Case No. IT-94-1-l, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 76 (Int'l Crim. Trib. for the former Yugoslavia Oct. 2, 1995) [hereinafter Tadić Decision on Defence Motion]. The seminal article on internationalization is Hans-Peter Gasser*, Internationalized Non-International Armed Conflicts: Case Studies of Afghanistan, Kampuchea, and Lebanon,* 33 AMERICAN UNIVERSITY LAW REVIEW 145 (1983). *See also* Christopher Greenwood, *International Humanitarian Law and the Tadić Case*, 7 EUROPEAN JOURNAL OF INTERNATIONAL LAW 265 (1996); Theodor Meron, *Classification of Armed Conflict in the Former Yugoslavia: Nicaragua's Fallout*, 92 AMERICAN JOURNAL OF INTERNATIONAL LAW 236 (1998).

3. For conflicting views on this subject, see HCJ 769/02 Public Committee against Torture in Israel v. Government of Israel 2006(2) PD 459 [2006] (Isr.), *reprinted in* 46 INTERNATIONAL LEGAL MATERIALS 373 (2007), *available at* http://elyon1.court.gov.il/files_eng/02/690/007/a34/02007690.a34.pdf; Hamdan v. Rumsfeld, 548 U.S. 557 (2006).

4. Clearly, the conflict between NATO (and other) forces and the Libyan security apparatus was international in character. The question is whether the recognition of the rebels (National Transitional Council) meant that NATO forces were now fighting on the side of the government against dissident armed forces (the remnants of the Libyan armed forces still loyal to Qaddafi) such that the conflict became non-international. On the recognition of the National transitional Council, see Stefan Talmon, *Recognition of the Libyan National Transitional Council,* AMERICAN SOCIETY OF INTERNATIONAL LAW INSIGHTS (June 16, 2011), http//www.asil.org/ insights110616.cfm.

This article explores these and other classification of cyber conflict issues.[5] Two caveats are in order. First, the occurrence of cyber operations in no way alters the classification of an ongoing kinetic conflict. The paradigmatic example is the cyber operations conducted by "patriotic hackers" during the 2008 international armed conflict between Georgia and Russia.[6] Second, this article will not consider the possible emergence of new categories of armed conflict, such as "transnational armed conflict."[7] Rather it adopts a conventional approach, one acknowledging two basic genre of conflict—international and non-international. To the extent cyber operations bear of classification, they do so within this generally accepted framework.

II. THE BASIC TYPOLOGY

The modern era of conflict classification began in 1949 with adoption of the four Geneva Conventions.[8] Earlier treaties governing hostilities had

5. On classification more generally, see Sylvain Vité, *Typology of Armed Conflicts in International Humanitarian Law: Legal Concepts and Actual Situations*, 91 INTERNATIONAL REVIEW OF THE RED CROSS 69 (2009); Jelena Pejic, *Status of Armed Conflicts*, *in* PERSPECTIVES ON THE ICRC STUDY ON CUSTOMARY INTERNATIONAL LAW 77 (Elizabeth Wilmshurst & Susan Breau eds., 2007).

6. On the Estonian and Georgian cases, see generally ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS (2010).

7. *See, e.g.*, Geoffrey Corn, *Hamdan, Lebanon, and the Regulation of Armed Conflict: The Need to Recognize a Hybrid Category of Armed Conflict,* 40 VANDERBILT TRANSNATIONAL LAW JOURNAL 295 (2006); Geoffrey S. Corn & Eric Talbot Jensen, *Untying the Gordian Knot: A Proposal for Determining Applicability of the Laws of War to the War on Terror*, 81 TEMPLE LAW REVIEW 787 (2008); Geoffrey S. Corn*, Making the Case for Conflict Bifurcation in Afghanistan*, *in* THE WAR IN AFGHANISTAN: A LEGAL ANALYSIS 181 (Michael N. Schmitt ed., 2009) (Vol. 85, U.S. Naval War College International Law Studies). For a well-reasoned piece suggesting a category of "extra-State" armed conflict, see Roy Schondorf, *Extra-State Armed Conflict: Is There a Need for a New Legal Regime?*, 37 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 1 (2004). The International Committee of the Red Cross has correctly rejected the notion of armed conflicts that are other than international and non-international. International Committee of the Red Cross, *How is the Term "Armed Conflict" Defined in International Humanitarian Law?* (Mar. 2008), http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf.

8. Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135;

been silent as to the conditions under which they applied. They merely assumed the existence of a "war."

Lassa Oppenheim set forth the classic definition of war in his 1906 treatise *International Law*: "War is a contention between two or more States through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases."[9] The critical element in the definition was that war must be between States. Intra-State conflict was principally a matter of domestic concern unless it rose to the level of a "belligerency."[10] Only then, and only because the conflict now resembled inter-State hostilities, did the law of war attach.

Oppenheim's definition implied that the existence of a war was a question of fact. The undeclared 1905 war between Japan and Russia brought this approach into question. In response to the conflict, the 1907 Second Hague Peace Conference adopted Hague Convention III relative to the Opening of Hostilities. In that instrument, State parties agreed that "hostilities between themselves must not commence without previous and explicit warning, in the form either of a declaration of war, giving reasons, or of an ultimatum with conditional declaration of war."[11] Consequently, a failure to declare war or the non-recognition of a state of war by a party to the conflict precluded application of treaties governing the conduct of hostilities.

Subsequent events discredited this formalistic approach. The Spanish Civil War illustrated the extent to which fratricidal violence could match that which occurred during inter-State conflict,[12] while the carnage of the Second World War highlighted the risk of leaving humanitarian law to the mercy of political decisions as to whether to declare war. Sensitive to these realities, the international community took a different tack in the 1949 Geneva Conventions. The approach taken in those instruments, which recog-

---

Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC I–IV respectively].

9. LASSA OPPENHEIM, II INTERNATIONAL LAW: A TREATISE 56 (1906).

10. UNITED KINGDOM MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 15.1.2 (2004). On belligerency, see Yair M. Lootsteen, *The Concept of Belligerency in International Law*, 166 MILITARY LAW REVIEW 109 (2000).

11. Convention No. III Relative to the Opening of Hostilities art. 1, Oct. 18, 1907, 36 Stat. 2259, T.S. No. 538, 1 Bevans 619.

12. Interestingly, parties to that conflict occasionally agreed to apply the norms set forth in the 1929 Geneva Convention on Prisoners of War. *See* Frédéric Siordet, *The Geneva Conventions and Civil War, in* III INTERNATIONAL REVIEW OF THE RED CROSS (Supp. to Nos. 8, 9 & 11) (Aug., Sept. & Nov. 1950).

nizes war in both the technical and material sense, has since matured into customary international law.[13]

The Geneva Conventions adopt a bifurcated scheme in Articles 2 and 3, which are "Common" to all four conventions. Common Article 2 sets forth the standard for international armed conflict. It provides that "the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them."[14] Reduced to basics, there are two key factual criteria for international armed conflict—a confrontation between States and hostilities that amount to "armed" conflict.

In 1949, Common Article 3 signaled a sea change in the international community's attitude towards internal conflagrations, for it represented the first *lex scripta* expressly applicable to non-international armed conflicts. By its terms, the article applies to an "armed conflict not of an international character occurring in the territory of one of the High Contracting Parties." As with Article 2, an armed conflict is a condition precedent to applicability, although the article does not address the nature of such a conflict in the non-international context. One point is clear, though. Given Common Article 2, a non-international armed conflict cannot involve hostilities between two or more States. Its applicability is resultantly limited to conflicts between a State and an armed group or those in which multiple armed groups are fighting each other.

In light of the many post-1949 conflicts, the International Committee of the Red Cross (ICRC) convened a Diplomatic Conference between 1973 and 1977 to "update" international humanitarian law. The Conference adopted two Protocols to the 1949 Geneva Conventions. Additional Protocol I addresses international armed conflict by reference to Article 2 of the 1949 Conventions.[15] Controversially, it also reaches "armed conflicts in which peoples are fighting against colonial domination and alien occupa-

13. For instance, guidance issued by States to their armed forces typically adopts this approach. *See, e.g.*, U.S. Navy, U.S. Marine Corps & U.S. Coast Guard, NWP 1-14M/MCWP 5-12/COMDTPUB P5800.7A, The Commander's Handbook on the Law of Naval Operations ¶¶ 5.1.2.1 & 5.1.2.2 (2007). On the notion of "war," see YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 3–15 (4th ed. 2005).

14. GC I-IV, *supra* note 8, Common art. 2. The article also extends applicability of the Conventions to occupation, even when uncontested.

15. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 1(3), June 8, 1977, 1125 U.N.T.S. 3.

tion and against racist regimes in the exercise of their right of self-determination."[16] Numerous States, most notably the United States, refused to become party to the instrument, in part due to this latter provision.[17]

Additional Protocol II applies to non-international armed conflicts. However, it sets a higher threshold of applicability than Common Article 3's naked reference to armed conflict that is not international. By Article 1, Protocol II applies

> to all armed conflicts which are not covered by Article 1 of [Additional Protocol I] and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol.[18]

The provision differs from Common Article 3 in its requirement that dissident or other armed forces control territory and its limitation to conflicts involving a State, thereby excluding non-international armed conflicts between organized armed groups. Importantly, Article 1 specifically excludes "situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts" from the ambit of non-international armed conflict.[19] This exclusion has been broadly accepted as reflective of customary international law in all non-international armed conflicts, a fact evidenced by its adoption in the Statute of the International Criminal Court.[20]

Taken together, this collage of provisions envisions four categories of conflict: 1) international armed conflict between States; 2) international

---

16. *Id*., art. 1(4).

17. INTERNATIONAL AND OPERATIONAL LAW DEPARTMENT, UNITED STATES ARMY JUDGE ADVOCATE GENERAL'S LEGAL CENTER AND SCHOOL, LAW OF WAR DOCUMENTARY SUPPLEMENT 232 (2011). *See also* Michael J. Matheson, *The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AMERICAN UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 419 (1987).

18. Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts art. 1(1), June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II].

19. *Id.*, art. 1(2).

20. Rome Statute of the International Criminal Court art. 8.2(d), July 17, 1998, 2187 U.N.T.S. 90. The statute is not limited to conflicts that meet the Additional Protocol II threshold.

armed conflict involving national liberation movements; 3) non-international armed conflict between a State and an organized armed group or between organized armed groups; and 4) non-international armed conflict at the Additional Protocol II level. The second and fourth categories are relevant only to application of Additional Protocols I and II respectively for Parties thereto. The first and third are acknowledged as customary categories of conflict.

III. INTERNATIONAL ARMED CYBER CONFLICT

As noted, international armed conflicts must be both "armed" and "international." The first criterion presents the quandary that cyber operations are not kinetic in nature and do not employ what would in common usage be considered as "weapons." At first glance, a conflict consisting of only cyber operations would, therefore, appear not to be "armed." Such a conclusion would be incongruous for cyber operations can have highly destructive, even deadly, results. A State involved in an exchange of cyber attacks at this level would be very likely to characterize the situation as international armed conflict, much as it would if it fell victim of another State's non-kinetic bacteriological attack.

The official ICRC *Commentary* to Article 2 provides that

> any difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of a state of war. It makes no difference how long the conflict lasts, how much slaughter takes place, or how numerous are the participating forces.[21]

The ICRC *Commentary* to Additional Protocol I is in accord:

> [H]umanitarian law . . . covers any dispute between two States involving the use of their armed forces. Neither the duration of the conflict, nor its

21. COMMENTARY TO GENEVA CONVENTION III RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 23 (Jean Pictet ed., 1960) [hereinafter GC III COMMENTARY]. *See also* Dietrich Schindler, *The Different Types of Armed Conflicts According to the Geneva Conventions and Protocols*, 163 RECUEIL DES COURS DE L'ACADEMIE DE DROIT INTERNATIONAL 131 (1979). *But see* Christopher Greenwood, *Scope of Application of Humanitarian Law*, *in* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 37, 48 (Dieter Fleck ed., 2d ed. 2009).

> intensity, play a role: the law must be applied to the fullest extent required by the situation of the persons and the objects protected by it.[22]

Adopting the same approach, the ICTY has defined armed conflict as the "resort to armed force between States" without recognizing any threshold for the duration or intensity of hostilities.[23]

By these standards, the concept of armed conflict implies forceful acts at whatever level.[24] *A fortiori*, any cyber operation that amounts to an "attack" in international humanitarian law terms would qualify as armed. Article 49(1) of Additional Protocol I defines attacks as "acts of violence against the adversary, whether in offence or defence." Although cyber operations are not violent in themselves, they can nonetheless generate violent consequences. To the extent that they result in injury or death of persons or damage or destruction of property, they are attacks satisfying the armed criterion of armed conflict.[25] For instance, if a State was behind the 2010 "Stuxnet" attack against supervisory control and data acquisition systems upon which the power centrifuges at an Iranian nuclear power plant depended, it would meet this threshold because physical damage resulted.[26]

---

22. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 62 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1988) [hereinafter AP COMMENTARY].

23. Tadić Decision on Defence Motion*, supra* note 2, ¶ 70.

24. It should be noted that an armed conflict can exist even in the absence of uses of force. For instance, Common Article 2 of the four 1949 Geneva Conventions extends to "all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance."

25. *See, e.g.*, Michael N. Schmitt, *Cyber Operations and the Jus in Bello, in* INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 89, 92–94 (Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies). It has been suggested that operations falling below the threshold may also qualify. INTERNATIONAL COMMITTEE OF THE RED CROSS, REPORT 31IC/11/5.1.2, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS 37 (2011) [hereinafter ICRC REPORT]; Knut Dörmann, *Applicability of the Additional Protocols to Computer Network Attacks* 6 (Nov. 19, 2004), http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf (paper delivered at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm). The issue is addressed at length in the TALLINN MANUAL ON THE INTERNATIONAL LAW OF CYBER WARFARE (Michael N. Schmitt ed., 2013). The author is grateful to his colleagues on the project leading to the *Manual* for their insights, many of which find reflection in this article.

26. The question remains as to whether a State was behind the operation.

But might a cyber operation by one State against another that does not cause physical injury or damage nevertheless initiate an armed conflict? The ICRC has taken the position that a cyber operation that "disables" an object is also an attack even when it does not cause physical damage.[27] This is a reasonable extension of the notion of damage, at least to the extent repair (as distinct from merely reloading software) of the cyber infrastructure concerned is necessitated. Since the operation is an attack, it is also armed in terms of qualification for armed conflict. That said, a *de minimis* standard should attach. In much the same way that a soldier throwing a rock across the border does not propel the States concerned into international armed conflict, it would not suffice, for instance, to merely disable a single computer that performs non-essential functions.

Beyond these cases, it is unclear where State practice will lead. Consider a situation in which a State takes control of critical infrastructure in another State, conducts denial-of-service attacks against essential societal services, or begins deleting or changing data in a manner that severely disrupts another State's economy. As perceptively noted by the ICRC, "[i]t would appear that the answer to these questions will probably be determined in a definite manner only through future state practice."[28]

In addition to being armed, cyber attacks must be of an "international" nature to qualify as international armed conflict. The term international denotes actions conducted by, or attributable to, a State. By the plain text of the provisions cited above, those conducted by a State's armed forces qualify. Although not mentioned in those provisions, it is beyond dispute that cyber attacks conducted by other organs of a State, such as intelligence or law enforcement agencies, also qualify.[29]

As noted by the ICTY in *Tadić*, "private individuals acting within the framework of, or in connection with, armed forces, or in collusion with

27. ICRC REPORT, *supra* note 25, at 37.

28. *Id.*

29. Draft Articles on Responsibility of States for Internationally Wrongful Acts, Rep. of the Int'l L. Comm'n, 53d Sess., GAOR 56th Sess., Supp. No. 10, U.N. DOC. A/56/10 (2001), *reprinted in* [2001] 2 YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 32, U.N. DOC. A/CN.4/SER.A/2001/Add.1 (Part 2) [hereinafter Articles of State Responsibility]. Article 4(2) of the Articles of State Responsibility provides that an "organ includes any person or entity which has that status in accordance with the internal law of the State."

State authorities may be regarded as de facto State organs."[30] Any cyber attacks they launch would be treated as if launched by *de jure* State organs. Cyber attacks carried out by a person or entity that, although not an organ of the State, is "empowered by the law of that State to exercise elements of the governmental authority . . . provided the person or entity is acting in that capacity in the particular instance" would likewise suffice.[31] An example would be a private corporation that a State authorizes by law to conduct cyber operations on its behalf, so long as the operations in question are of the sort for which said authorization was granted.

More problematic in terms of qualifying as international are activities engaged in by individuals or groups that are neither organs of a State nor authorized to act on its behalf. It appears clear that cyber attacks by individuals or groups acting *sua sponte* are generally not attributable to a State for the purpose of finding an international armed conflict. The classic example is the "hacktivist" cyber campaign against Estonia in 2007 (moreover, they were not "armed").[32] However, if a State endorses and encourages the perpetuation of the cyber operations, the individuals or groups involved will be deemed "de facto organs" of the State, such that the activity meets the international criterion. This principle was enunciated (albeit, in the State responsibility context) by the International Court of Justice in the *Hostages* case and cited with approval by the ICTY in *Tadić* when dealing with attribution for the purposes of conflict classification.[33]

Consider, for example, a case in which a group of one State's nationals conduct cyber attacks against another State. If the government of the first State announces its approval of the attacks and takes steps to perpetuate the attacks, as in the case of establishing cyber defense mechanisms that preserve the group's ability to continue its attacks, the group becomes a *de facto* State organ even if that State did not originally provide direction to the group.

A scenario in which some relationship exists between a State and the individuals or group conducting the cyber attacks is more likely. The ICTY

---

30. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Chamber Judgment, ¶ 144 (Int'l Crim. Trib. for the former Yugoslavia July 15, 1999) [hereinafter Tadić Appeals Chamber Judgment].

31. Articles of State Responsibility, *supra* note 29, art. 5.

32. See generally the discussion of these incidents in TIKK, KASKA & VIHUL, *supra* note 6.

33. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, ¶ 74 (May 24); Tadić Appeals Chamber Judgment, *supra* note 30, ¶¶ 133–37.

addressed this situation head on in *Tadić* when assessing whether the conflict in Bosnia-Hercegovina was international by virtue of the relationship between the Bosnian Serb armed groups and the Serb-dominated Federal Republic of Yugoslavia. In an often-overlooked distinction, the Tribunal took different approaches to the actions of organized armed groups (defined below) and individuals.

As to the former, the ICTY held that the correct threshold was one of "overall control going beyond the mere financing and equipping of such forces and involving also participation in the planning and supervision of military operations."[34] The issuance of specific orders or instructions relating to a single operation is not required. To illustrate, a State that exercises control over a group sufficient to allow it to direct the group to mount (or to desist from mounting) a broad campaign of cyber attacks exercises overall control. Similarly, if a State instructs the group to attack, or refrain from attacking, a particular category of cyber targets (as distinct from specific targets), it enjoys overall control of the group. But note the Tribunal's mention of equipping the group. Merely providing software or hardware with which attacks are conducted does not suffice to attribute a group's actions to the State for the purpose of finding an international armed conflict (although such assistance may violate certain norms of international law).

The requisite degree of control over the actions of individuals who conduct cyber attacks without being members of an organized armed group is much higher. In such cases, the State must issue "specific instructions or directives aimed at the commission of specific acts" before attribution of the acts to the State for the purpose of classifying the conflict as international occurs.[35] Absent such instructions, the attacks cannot be attributed to the State for that purpose. Neither would the conflict be non-international since, as will be discussed, the individuals do not comprise an organized armed group.

---

34. Tadić Appeals Chamber Judgment, *supra* note 30, ¶ 145. See also *Lubanga*, where the International Criminal Court described overall control as "a role in organising, coordinating, or planning the military actions of the military group." Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Decision on Confirmation of Charges, ¶ 211 (ICC Jan. 29, 2007) [hereinafter *Lubanga*]. In the *Genocide* case, the International Court of Justice observed that the overall control test "may well be . . . applicable and suitable." Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. and Montenegro), 2007 I.C.J. 43, ¶ 404 (Feb. 26).

35. Tadić Appeals Chamber Judgment, *supra* note 30, ¶ 132.

Should a State permit cyber attacks to take place from its territory, it may be in breach of its international legal obligation to "police" its territory in order to ensure it is not used for purposes harming other States.[36] Yet, its tolerance of the attacks does not satisfy the international criterion unless, as mentioned, the State goes further. It is irrelevant whether the attacks in question are mounted by a single individual or, as in the Estonian case, hundreds of persons.

Finally, it is sometimes questioned whether attribution to a State is required at all for qualification as an international armed conflict. In the *Targeted Killing* case, the Israeli Supreme Court argued that attribution is not necessary so long as the group in question operates transnationally, that is, the conflict "crosses the borders of the state."[37] In the cyber context, this situation is highly probable, for organized armed groups might well launch cyber attacks from relative safety abroad. The U.S. Supreme Court took a contrary approach in *Hamdan*, where it found that the conflict with the Al-Qaeda terrorist organization was "not of an international character" because it was not between States.[38] In light of the earlier discussion, the U.S. position on this particular point is better reasoned.

IV. NON-INTERNATIONAL ARMED CYBER CONFLICT

Common Article 3 to the Geneva Conventions defines non-international armed conflicts in the negative as those that are "not of an international character."[39] The ICTY has further developed the notion of non-international conflict. In *Tadić,* the Tribunal described such conflicts as "protracted armed violence between governmental authorities and orga-

36. The International Court of Justice affirmed this principle in its first case, *Corfu Channel*. The Court held that every State has an "obligation to not allow knowingly its territory to be used for acts contrary to the rights of other States." Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22 (Apr. 9).

37. Public Committee against Torture in Israel, *supra* note 3, ¶ 18.

38. Hamdan, *supra* note 3, 628–32 (2006).

39. GC I–IV, *supra* note 8, Common art. 3 ("In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply, as a minimum, the following provisions. . . ."). Only States can be High Contracting Parties. On non-international armed conflict generally, see ANTHONY CULLEN, THE CONCEPT OF NON-INTERNATIONAL ARMED CONFLICT IN INTERNATIONAL HUMANITARIAN LAW (2010); EVE LA HAYE, WAR CRIMES IN INTERNAL ARMED CONFLICTS (2008); LINDSAY MOIR, THE LAW OF INTERNAL ARMED CONFLICT (2002).

nized armed groups or between such groups within a State."[40] The equivalent definition has been adopted by international tribunals and in the Statute of the International Criminal Court.[41] Additional Protocol II also refers to a conflict between a State's armed forces "and dissident armed forces or other organized armed groups." Accordingly, two essential criteria apply for all non-international armed conflicts—participation by an organized armed group and a particular level of intensity.

Organized armed groups must be both "organized" and "armed." Common Article 3 refers to "parties to a conflict," a reference that serves as the source of the organization requirement. In considering this requirement, the ICTY has noted

> some degree of organisation by the parties will suffice to establish the existence of an armed conflict. This degree need not be the same as that required for establishing the responsibility of superiors for the acts of their subordinates within the organization, as no determination of individual criminal responsibility is intended under this provision of the Statute.[42]

But the group must nevertheless be organized. Organization allows for acting in a coordinated manner, thereby generally heightening the capability to engage in violence. In military operations, such coordination typically involves mission planning, sharing intelligence, and exercising command and control. In other words, the organization criterion implies that the actions are best understood as those of a group and not its individual members. This structural requirement is fundamental, for absent structure there is no identifiable enemy to treat as the other party to the conflict.[43]

Whether a group is organized is always a fact and context specific determination. In *Limaj*, the ICTY looked to such factors as, *inter alia*, the existence of a formal command structure, the creation of unit zones of opera-

---

40. Tadić Decision on Defence Motion, *supra* note 2, ¶ 70.

41. Prosecutor v. Akayesu, Case No. ICTR-96-4-T, Judgment, ¶ 619 (Sept. 2, 1998); Prosecutor v. Rutaganda, Case No. ICTR-96-3-T, Judgment, ¶ 92 (Dec. 6, 1999); Prosecutor v. Fofana, Case No. SCSL-2004-14-AR73, Decision on Appeal Against "Decision on Prosecution's Motion for Judicial Notice and Admission of Evidence," ¶ 32 (May 16, 2005) (Robertson, J., separate opinion); *Lubanga*, *supra* note 34, ¶ 233; Prosecutor v. Bemba Gombo, Case No. ICC-01/05-01/08, Decision on Confirmation of Charges, ¶ 229 (June 15, 2006); Rome Statute, *supra* note 20, art. 8(2)(f).

42. Prosecutor v. Limaj, Case No. IT-03-66-T, Judgment, ¶ 89 (Int'l Crim. Trib. for the former Yugoslavia Nov. 30, 2005) [hereinafter *Limaj*].

43. For instance, in order to open termination of conflict negotiations.

tion, the issuance of orders, the establishment of a headquarters and the promulgation of disciplinary orders to find that the Kosovo Liberation Army qualified as an organized armed group in its conflict with the Federal Republic of Yugoslavia.[44]

What is clear is that individuals acting alone that conduct cyber attacks against a State (or a particular armed group) cannot meet the organized criterion. For example, despite the number of hacktivists involved in the cyber operations against Estonia, they lacked the requisite degree of organization and therefore the operations did not amount to non-international armed conflict. Similarly, consider a case in which a website containing malware and listing potential cyber targets is accessed by large numbers of individuals who are unaffiliated with the creator of the website. Those individuals who do so do not qualify as an organized armed group; they lack the requisite structure. When cyber attacks are merely collective in the sense of occurring in parallel, they are not organized.

Cyber attacks conducted by a group that organizes entirely on-line are more difficult to classify. The members of virtual organizations may never meet nor even know each other's actual identity. Nevertheless, such groups can act in a coordinated manner against the government (or an organized armed group), take orders from a virtual leadership and be highly organized. For example, one element of the group might be tasked to identify vulnerabilities in target systems, a second might develop malware to exploit those vulnerabilities, a third might conduct the operations and a fourth might maintain cyber defenses against counter-attacks.

The primary obstacle to characterization of the group as organized would be its inability to enforce compliance with international humanitarian law. Additional Protocol II imposes a requirement that a group be "under responsible command" before a non-international armed conflict covered by the instrument exists.[45] This requirement should not be interpreted too strictly. As noted in the ICRC *Commentary* to the article, the term

> implies some degree of organization of the insurgent armed group or dissident armed forces, but this does not necessarily mean that there is a hierarchical system of military organization similar to that of regular armed forces. It means an organization capable, on the one hand, of planning

44. *Limaj*, *supra* note 42, ¶¶ 94–129.
45. AP II, *supra* note 18, art. 1(1).

> and carrying out sustained and concerted military operations, and on the other, of imposing discipline in the name of a de facto authority.[46]

In a virtually organized group, the requirement of an ability to carry out sustained and concerted military operations could be met to the extent that cyber operations are equated with military operations, which, as discussed, is the case. However, imposing discipline would be difficult since the group lacks physical control over its members.

Complicating matters is Additional Protocol II's requirement that the group be able "to implement this Protocol." [47] The phrase is generally understood as an ability to comply with and enforce international humanitarian law. Before violence can qualify as a Protocol II conflict, "the parties may reasonably be expected to apply the rules developed in the Protocol, since they have the minimum infrastructure required therefor."[48] While there is no requirement that the law actually be enforced, the group must be organized so as to enable enforcement. In a virtually organized group, such organization is lacking since there is no physical connection between the members.

It must be cautioned that since this treaty law requirement derives from Additional Protocol II, it is only applicable in and of itself to conflicts in which that instrument applies. Common Article 3 contains no equivalent condition, thereby raising the question of whether an analogous customary law norm applies to conflicts other than Additional Protocol II non-international armed conflicts. In this regard, the commentary to Article 3 notes that the Diplomatic Conference that drafted the 1949 Geneva Conventions considered setting express preconditions for such conflicts. Although the proposal was rejected, the *Commentary* asserts that they "constitute convenient criteria."[49] The first condition was that the "Party in revolt against the *de jure* Government possesses an organized military force, an authority responsible for its acts, acting within a determinate territory and having the means of respecting and ensuring respect for the Convention."[50] It would appear reasonable, therefore, to extend the Additional Protocol II requirements regarding responsible command (vis-à-vis enforcing disci-

46. AP COMMENTARY, *supra* note 22, ¶ 4663.

47. AP II, *supra* note 18, art. 1(1).

48. AP COMMENTARY, *supra* note 22, ¶ 4470.

49. COMMENTARY ON GENEVA CONVENTION I FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND SICK IN THE ARMED FORCES IN THE FIELD 49 (Jean Pictet ed., 1952).

50. *Id.*

pline) and an ability to implement international humanitarian law to all non-international armed conflicts. The ICTY adopted this approach in *Boskoski*[51] and it is consistent with the principle of command responsibility in non-international armed conflicts.[52] If valid, the extension to all non-international armed conflicts would preclude virtually organized groups from qualifying as organized armed groups for the purpose of classifying a conflict as non-international.

In addition to being organized, the group in question must be armed. The meaning of armed in the non-international armed conflict context parallels that attending international armed conflict. As discussed, it generally presumes the conduct of "attacks." Yet, since non-international armed conflict is premised on the activities of a group, as distinct from a State, the question of attribution of an individual member's conduct to the group as a whole arises. Since it is the group that must be armed, the group itself must have a purpose of carrying out armed activities. If individual members of an organized group carry out cyber attacks on their own accord, that is, not on behalf of the group, the group does not meet the armed criterion.

In contradistinction to international armed conflict, non-international armed conflict entails a certain degree of intensity. Recall that riots, civil disturbances, or isolated and sporadic acts of violence do not suffice; the hostilities must also be protracted. Decisions of the ICTY have cited such factors as the gravity of the attacks, the collective character of the hostilities, the need to increase forces to deal with the situation, the time over which the hostilities have taken place, and whether the United Nations Security Council has addressed the matter as bearing on whether the intensity threshold is satisfied.[53] However, no bright-line intensity test exists, nor is there any clear standard for "protracted" conflict.[54] In light of the manner

51. Prosecutor v. Boskoski, Case No. IT-04-82-T, Judgment, ¶ 205 (Int'l Crim. Trib. for the former Yugoslavia July 10, 2008).

52. Although responsible command and command responsibility are separate legal concepts, it would be illogical to impose command responsibility on an individual for the actions of individuals who are members of a group that are not under responsible command; the concepts are therefore different, but related. On the issue, see Prosecutor v. Hadzihazanovic, Case No. IT-01-47-AR72, Appeals Chamber Decision on Interlocutory Appeal Challenging Jurisdiction in Relation to Command Responsibility, ¶¶ 16–22 (Int'l Crim. Trib. for the former Yugoslavia July 16, 2003).

53. Prosecutor v. Haradinaj, Case No. IT-04-84-T, Judgment, ¶ 49 (Int'l Crim. Trib. for the former Yugoslavia Apr. 3, 2008) (summarizing various indicative factors).

54. In *Abella*, the Inter-American Commission on Human Rights characterized a thirty-hour clash between dissident armed forces and the Argentinian military as non-

in which cyber campaigns are mounted, it must be noted that although cyber attacks have to be frequent enough to be considered related, they clearly do not have to be continuous.

This is a high threshold that would preclude many cyber operations from sufficing for the purpose of finding a non-international armed conflict. Even highly destructive cyber attacks would fail to qualify unless they occurred on a regular basis over time. They would instead be addressed within the criminal law paradigm and be governed internationally by human rights, not humanitarian, law.

One issue that is somewhat murky is the classification status of cyber attacks conducted by an organized armed group during an international armed conflict between two States. It is clear that if a group "belongs to" a party to the conflict, the conflict remains wholly international in character. The concept of belonging to, which stems from Article 4 of Geneva Convention III, implies at least some de facto relationship between the group and a State that is a party.[55] The article's commentary suggests that even tacit agreement is sufficient so long as it is clear for which side the group is fighting.[56]

Much more complicated is the situation in which a group engages in cyber attacks without doing so on behalf of one of the parties to an international armed conflict. This is not a remote hypothetical. For instance, when the conflict in Iraq was still international in character, organized armed groups lacking any connection with the Baathist regime attacked coalition forces. The groups, such as the Shia militia, were opposed to both sides during that conflict. An analogous situation could easily arise in which a group mounts cyber attacks against a party *sua sponte*.

The ICRC's *Interpretive Guidance on the Notion of Direct Participation in Hostilities* addresses such situations. It contends that "organized armed groups operating within the broader context of an international armed conflict without belonging to a party to that conflict could still be regarded as parties to a separate non-international armed conflict."[57] Some participants in the expert process that resulted in the *Guidance* rejected the ICRC's position

---

international armed conflict. Abella v. Argentina, Case 11.137, Inter-Am. Comm'n H.R., Report No. 55/97, OEA\Ser.L\V\II.98, doc. 6 rev. ¶¶ 148, 327 (1998).

55. GC III, *supra* note 8, art. 4A(2).

56. GC III COMMENTARY, *supra* note 21, at 57.

57. NILS MELZER, INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION UNDER INTERNATIONAL HUMANITARIAN LAW 24 (2009).

on the basis that it would prove problematic in practice because it requires application of the law of both international and of non-international armed conflict in the same battlespace.[58] In their view, it was more appropriate to ask whether an unambiguous nexus existed between the actions of the group in question and the international armed conflict, rather than any party thereto. For instance, an organized armed group might conduct cyber attacks against an occupying force because of religious or political opposition to the occupants, not to expel them on behalf of the government. The requisite nexus between the group and the conflict would be their opposition to the occupation. In such a case, the conflict would remain entirely international irrespective of the lack of a relationship between the group and the occupied State.

Finally, recall that Additional Protocol II only applies when organized armed groups control territory. Since a group cannot control territory without physical presence, the instrument is generally thought to be inapplicable to cyber-only conflicts. It would accordingly only apply to cyber operations in those Additional Protocol II conflicts involving an organized armed group that controls territory and conducts such operations.

V. CONCLUSION

To date, States have refrained from characterizing any cyber operations conducted outside the context of an on-going armed conflict as either international or non-international armed conflict. Be that as it may, cyber operations will in the future inevitably present difficult conflict classification challenges for States. With regard to international armed conflict, attribution of cyber operations conducted by non-State actors will likely prove even more problematic than the attribution to States of kinetic actions has been in the past. In the context of non-international armed conflict, qualification as an organized armed group will prove increasingly complex as the structures, means and prevalence of virtual organization grow and evolve. Perhaps most importantly, the approach taken in this article to the interpretation of the term "armed" is, although presently reflecting *lex lata*, unlikely to survive. With States and non-State actors engaging in ever more destructive and disruptive cyber operations and societies becoming deeply dependent on the cyber infrastructure, State practice accompanied by *opinio juris* can be expected to result in a lowering of the current threshold. The

58. Based on author's participation.

law of cyber armed conflict is a work in progress and will remain so for the immediate future.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?

Noam Lubell

89 INT'L L. STUD. 252 (2013)

Volume 89 2013

Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?

Noam Lubell[*]

I. INTRODUCTION

Most of the advanced and largest militaries in the world have, in recent years, devoted significant attention and resources to the development of the capacity to conduct—and defend against—cyber operations.[1] Indeed, cyber operations feature prominently in discussions over future conflicts and are expected to be an inherent and major component in the waging of war. But cyber operations are not usually conducted with the aim of straightforward material harm to a physical military object and their use

* Reader in Law, School of Law, University of Essex, United Kingdom. Thanks are due to Marty Ehlenbach for research assistance and to Audrey Guinchard for comments.

1. U.S. Department of Defense, Department of Defense Strategy for Operating in Cyberspace (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf; HM Government, Securing Britain in an Age of Uncertainty: UK Strategic Defence and Security Review (2010), *available at* http://www.cabinetoffice.gov.uk/sites/default/files/resources/strategic-defence-security-review.pdf; NATO Cooperative Cyber Defence Centre of Excellence, http://www.ccdcoe.org/; Jim Wolf, *China Cyber Capability Puts U.S. Forces at Risk: Report*, REUTERS (Mar. 8, 2012, 12:11 AM), http://www.reuters.com/article/2012/03/08/us-china-usa-cyberwar-idUSBRE8270AF20120308; Nick Hopkins, *Militarisation of Cyberspace: How the Global Power Struggle Moved Online*, GUARDIAN (Apr. 16, 2012, 10:00 AM), http://www.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle.

raises complex questions concerning the choice of targets. During armed conflict, international law provides detailed rules on targeting, most of which stem from the fundamental principle of distinction. At its most basic understanding, this rule requires that all things and people military must be distinguished from things and people civilian.[2] It governs questions of who and what may be attacked. It also influences other rules on how attacks may be carried out—prohibitions of indiscriminate attacks and concepts of proportionality would in most cases become meaningless without the distinction between military and civilian.[3] The principle of distinction is one of the foundations of the law of war. The International Court of Justice has described it as part of "[t]he cardinal principles contained in the texts constituting the fabric of humanitarian law."[4] As such, this principle should presumably hold true in any type of conflict. The cyber sphere, however, presents unique challenges to our ability to adequately distinguish between military and civilian and thereby adhere to this fundamental principle. Moreover, the nature of cyber operations is such that it does not neatly fit into the paradigm of hostilities around which the law of armed conflict (LOAC) is constructed. In fact, it has even been debated whether the LOAC rules on targeting would always apply to cyber operations, and whether the need to distinguish between military and civilian and the prohibition on attacking civilian targets are applicable to all forms of cyber operations or not.[5] This article will examine these questions in the following manner. Part II will address the question of the nature of cyber operations

---

2. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 48, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

3. *Id.*, art. 51 (protection of the civilian population).

4. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 78 (July 8) [hereinafter *Nuclear Weapons*]. Note also the International Committee of the Red Cross commentary on the rule, which states the rule of protection and distinction is

> the foundation on which the codification of the laws and customs of war rests: the civilian population and civilian objects must be respected and protected in armed conflict, and for this purpose they must be distinguished from combatants and military objectives. The entire system established in The Hague in 1899 and 1907 and in Geneva from 1864 to 1977 is founded on this rule of customary law.

COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 1863 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987) (footnotes omitted) [hereinafter COMMENTARY ON THE ADDITIONAL PROTOCOLS].

5. *See infra* pp. 254.

that are likely to take place. This will include an examination of cyber operations as fitting within the notion of attack. Part III will then turn to an analysis of the appropriate threshold of harm that would lead a cyber operation to be considered an attack under LOAC—and thus subject to the principle of distinction—with particular focus on destruction of data and harm that does not have direct physical manifestation.

II. THE CONCEPT OF ATTACK IN CYBER OPERATIONS

In order to examine what might be lawful targets in the context of cyber operations, we must first get an idea of what types of targets the parties to a conflict might seek to attack. Actual cyber operations in past years range from hacking into government or military networks, such as the "Titan Rain" incident in 2003 when U.S. Department of Defense facilities, NASA labs, Lockheed Martin and other systems were hacked into and lost many terabytes of information (Chinese sources were alleged to have been behind this operation)[6] through to more recent years and well-publicized cyber incidents directed against Estonia and Georgia, which included incidents described as denial of service attacks leading to severe disruption of media, government and banking systems.[7] The Stuxnet worm is alleged to have led to physical damage to centrifuges at the Iranian nuclear facilities.[8] Cyber operations have also been employed in tandem with kinetic attacks, as was said to have happened in the Israeli attack on an alleged nuclear development site in Syria.[9] Individuals with a personal agenda have demonstrated the dangerous potential for using computer networks to gain con-

6. RICHARD A. CLARKE & ROBERT KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 58, 125–26 (2010). There have been a number of other such incidents originating from various sources, including those known as "Solar Sunrise" and "Moonlight Maze," as well as Operation "Buckshot Yankee." For the latter, see Ellen Nakashima, *Cyber-Intruder Sparks Massive Federal Response—and Debate over Dealing with Threats*, WASHINGTON POST (Dec. 9, 2011), http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html. For a detailed list of these and other cyber operation incidents, see H. HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR app. 1 (2012).

7. See the detailed discussion in ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS (2010).

8. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES, June 1, 2012, at A1.

9. CLARKE & KNAKE, *supra* note 6, at 1–8.

trol of complex systems and unleash serious damage.[10] More generally, cyber attacks are described as operations seeking to accomplish a wide range of effects, including "[d]estroy data on a network or a system connected to the network";[11] "[b]e an active member of a network and generate bogus traffic";[12] "[c]landestinely alter data in a database stored on the network";[13] and "[d]egrade or deny service on a network."[14]

One way of describing all of this is simply to say that targets in cyber operations are usually computer network systems. It is, however, also possible to create an element of differentiation between these potential targets. In certain operations, such as denial of service, it is the computer system itself that is the object of the operation and the direct objective is to shut down or prevent the system from functioning as designed.[15] Alternatively, it may be that the objective is the corruption of data on the system or the destruction of specific information data, in which case it might be more accurate to state that the target of the operation is not the system as a whole but rather the data.[16] Lastly, if an attack is designed to take control of a computer network in order to directly manipulate a physical object—for example, take control of a missile launch system or open the floodgates of a dam—then it might be more accurate to describe the computer network as part of the means and methods of attack, while the actual target is the physical object directly affected.

---

10. For example, see the case of an Australian individual who caused the dumping of sewage into rivers, leading to serious harm to the local environment. Robert O'Harrow Jr., *Search Engine Exposes Industrial-Sized Dangers*, WASHINGTON POST (June 4, 2012), http://www.washingtonpost.com/investigations/cyber-search-engine-exposes-vulnerabilities/2012/06/03/gJQAIK9KCV_story.html. In another case, a disgruntled employee disabled the system for detecting oil pipeline leaks off the Californian coast. David Kravets, *Feds: Hacker Disabled Offshore Oil Platforms' Leak-Detection System*, WIRED (Mar. 18, 2009, 3:47 PM), http://www.wired.com/threatlevel/2009/03/feds-hacker-dis/. *See also* Rebecca Allison, *Hacker Attack Left Port in Chaos*, GUARDIAN (Oct. 6, 2003), http://www.guardian.co.uk/technology/2003/oct/07/usnews.uknews.

11. Herbert S. Lin, *Offensive Cyber Operations and the Use of Force*, 4 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 63, 69–70 (2010).

12. *Id.*

13. *Id.*

14. *Id.*

15. For example, disrupting command and control systems, or communication networks.

16. See *infra* pp. 256 for an analysis of whether or not data should be considered as an object in the context of attacks.

Ultimately, since the world we actually live in is not the non-material cyber sphere, it is clear that any cyber operation is designed to lead—directly or indirectly—to a result which includes an effect in the physical world. Nonetheless, there is a qualitative difference between attacks designed to gain direct control of a physical object and cause it to act in a specific planned way, and attacks targeting the networks and data themselves, aiming for more generalized knock-on effects. In the former cases, such as using a computer network in order to gain control of an opposing party's missile system and cause it to fire upon itself, or a cyber operation designed to open a dam and unleash a flood, there is, of course, the need to assess the legality of these targets. For this determination of whether these are lawful targets under LOAC, such cyber operations may raise certain new aspects, but at the end of the day the legality question will in most cases not be unique to cyber operations.[17] It is in those circumstances in which the systems and data themselves are attacked where the more complex questions arise with regard to choice of target.

A number of legal concerns must be recognized. First and foremost is, of course, the question of whether certain computer network systems can be considered military objectives, and consequently lawful targets. Further challenges in this context concern the ability to take adequate precautions, avoid disproportionate effects, and not stray beyond lawful means and methods. These are all matters of vital importance, but are not within the scope of this article focused on lawful targets.[18] The issues addressed here

---

17. The LOAC rules most directly applicable include Article 56(1) of Additional Protocol I, which states that

> [w]orks or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population. Other military objectives located at or in the vicinity of these works or installations shall not be made the object of attack if such attack may cause the release of dangerous forces from the works or installations and consequent severe losses among the civilian population.

18. Cyber operations can present particular challenges in these areas due to characteristics such as their potential capacity to spread indiscriminately through the networks, and to have indirect effects that may be difficult to foresee. For a discussion of some of these issues, see Eric Talbot Jensen, *Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations?*, 18 AMERICAN UNIVERSITY INTERNATIONAL LAW REVIEW 1145 (2003); KNUT DÖRMANN, APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS 2–3 (2004), *available at* http://www.icrc.org/eng/resources/documents/misc/68lg92.htm. For an example of a unique challenge arising from cyber operations, see the discussion of active defenses and use of "hack back" in

are concerned with questions relating to the nature of the objects attacked and whether they must be defined as military objectives in order to be lawful targets of cyber operations. In other words, we are currently examining *what* can be attacked rather than *how/with what*.

Before proceeding further, a preliminary matter must be clarified: the question of lawful targets in the *ius in bello* is separate from the questions of the *ius ad bellum*. While the need for maintaining a separation between these two areas of law has long been evident for a number of reasons,[19] the discussions surrounding cyber operations have on occasion muddied the waters. Much of this is due to the fact that cyber operations present equally vexing problems for both bodies of law and, moreover, many of these challenges in both the *ius ad bellum* and the *ius in bello* surround the notion of "attack."[20] As has been the subject of much discussion, there is a debate as to whether cyber operations against certain objects might be considered an armed attack, thereby triggering the right to self-defense under the *ius ad bellum*.[21] However, the response to that question does not provide us with an answer as to whether the object was a lawful target under the *ius in bello*; the debate over defining an attack as an armed attack under the *ius ad bellum* can exist regardless of the military nature of the object attacked. An event constituting an armed attack for the purpose of the *ius ad bellum* might include an attack against the military installation of another State, but equally if the attack was against a civilian target (e.g., bombing civilian areas of a city) this would also be an armed attack under the *ius ad bellum*. A determination of an armed attack having occurred tells us therefore nothing about the civilian or military nature of the object attacked—a criterion crucial to

---

David E. Graham, *Cyber Threats and the Law of War*, 4 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 87, 101–2 (2010).

19. For example, the application of the *ius in bello* must not be linked to determinations under the *ius ad bellum* in order to ensure equal application of the *ius in bello* rules, thus alleviating the risk of dis-incentivizing one of the parties from adhering to the rules. It is also notoriously difficult to agree on violations of the *ius ad bellum*, making any reliance on *ius ad bellum* determinations for the purpose of *ius in bello* rules a sure recipe for disaster.

20. For attack in the context of the *ius in bello,* see the detailed discussion *infra* pp. 262. For the *ius ad bellum*, see the authorities *infra* note 21.

21. For discussion of the *ius ad bellum* in the context of cyber operations, *see*, *e.g.*, Matthew Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421 (2011); Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885 (1999); TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE ch. II (The Use of Force) (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

the determination of lawful targets under the *ius in bello*. Accordingly, the current focus is not on the *ius ad bellum*, but on the nature of lawful targets within the *ius in bello*.

Another vital differentiation—and one which requires clarification—is the significance of using the word "attack." As noted above, under the *ius ad bellum*, the key is whether a specific event meets the threshold of an *armed* attack. This allows for perhaps a looser usage of the phrase "cyber attacks" in the knowledge that this phrase does not in itself contain a legal determination as to whether it constitutes an *armed* attack under the *ius ad bellum*. This, however, is not the case for *ius in bello*, where—as will be seen shortly—the very use of the word "attack" may in and of itself have significant legal repercussions, including for the issue of lawful targets during these operations. For the sake of legal clarity, it would therefore be advisable to utilize a more legally neutral (at least under the *ius in bello*) description and—unless intending to define an event as an attack under LOAC—to speak of cyber operations rather than cyber attacks.[22] This has not, unfortunately, been the case thus far. In fact, it appears that the term "cyber attack" has been used indiscriminately when discussing a wide range of operations, including activities such as hacking into Google servers or probing government computers,[23] and defacing websites.[24] Indeed, the U.S. Department of Defense defines the phrase "computer network attack" as "[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[25] This definition—or

22. This is reminiscent of another area of LOAC in which terms are used without due regard to their legal implications, most notably in the inaccurate use of the term "combatant" to describe any fighter, even though the individual described might not meet the strict definition for being a combatant as set out in the law. For an examination of the difference between rhetoric, factual descriptions and legal terms in this latter context, see NOAM LUBELL, EXTRATERRITORIAL USE OF FORCE AGAINST NON-STATE ACTORS ch. 6 (2010).

23. Eric Talbot Jensen, *Cyber Warfare and Precautions against the Effects of Attacks*, 88 TEXAS LAW REVIEW 1533, 1536–42 (2010).

24. "The Federal Bureau of Investigation (FBI) reports that cyberattacks attributed to terrorists have largely been limited to unsophisticated efforts such as e-mail bombing of ideological foes, denial-of-service attacks, or defacing of websites." CATHERINE A. THEOHARY & JOHN ROLLINS, CONGRESSIONAL RESEARCH SERVICE, R41674, TERRORIST USE OF THE INTERNET: INFORMATION OPERATIONS IN CYBERSPACE 5 (2011), *available at* http://assets.opencrs.com/rpts/R41674_20110308.pdf.

25. *Computer Network Attack*, *in* DOD DICTIONARY OF MILITARY AND ASSOCIATED TERMS (Nov. 8, 2010), http://www.dtic.mil/doctrine/dod_dictionary/.

similar versions—has also been used by commentators writing on the topic.[26] Notably, it is a wide definition that can encompass a vast array of cyber operations with many different types of targets and varying degrees of effects. Moreover, it includes cyber operations designed to damage data, not just physical destruction.[27]

The dangerous ease with which we use the word "attack" causes us to unwittingly slide into an assumption that all these so-called attacks require an analysis under LOAC. But this is not always the case. There can be plenty of cyber operations that occur outside the context of an armed conflict, such as certain types of cyber espionage between supposedly friendly countries to which the law of armed conflict would not apply.[28] The inapplicability of LOAC in many situations is a crucial matter which must not be cast aside without consideration. Once the LOAC framework enters the stage, the legal regulation of operations takes on a new dimension that has significant repercussions for all concerned.[29] This is not an exhortation to never apply LOAC, but simply a reminder that it does not become applicable purely because we use the word "attack." LOAC can only apply within situations that qualify as an armed conflict. There is a complex debate as to whether stand-alone cyber operations between two parties—devoid of the kinetic actions usually associated with hostilities—can ever be considered an armed conflict.[30] This, however, becomes less of an obstacle if the cyber

26. DINNISS, *supra* note 6, at 4. Having used this definition, Dinniss later in the same book notes two different concepts of attack: "the question is raised as to when a computer network attack becomes an attack for the purposes of international humanitarian law." *Id.* at 179. *See also* Lin, *supra* note 11, at 63.

27. This point will be returned to later in the examination of data as an "object" of attack.

28. *See infra* notes 81–88 and accompanying text for mention of other relevant bodies of law which may regulate cyber operations outside of armed conflict.

29. For example, it can permit attacks that lead to civilian casualties that might otherwise have been unlawful. Equally, however, if violating the LOAC rules, those conducting the attacks will be open to charges under international criminal law.

30. This will largely depend on the manifestation and consequences of the cyber operations. See discussion in Noam Lubell, *Cyber Warfare as Armed Conflict*, *in* BRUGES COLLOQUIUM, TECHNOLOGICAL CHALLENGES FOR THE HUMANITARIAN LEGAL FRAMEWORK 41 (College of Europe & International Committee of the Red Cross eds., 2011), *available at* http://www.coleurope.eu/sites/default/files/uploads/page/collegium_41_0.pdf; Michael N. Schmitt, *Cyber Operations and the* Jus in Bello*: Key Issues*, *in* INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 89, 102–6 (Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies); DÖRMANN, *supra* note 18, at 2–3. At least in theory, the possibility does exist as "the International Group of Experts unanimously concluded that cyber operations alone

operations are conducted alongside traditional methods of warfare.[31] The current focus of this article is on circumstances in which cyber operations take place between parties to an existing armed conflict and in which, therefore, LOAC has already been triggered.

The need for concern over the correct use of the term "attack" becomes evident when considering the repercussions of cyber operations that take place during armed conflict but might not, arguably, constitute an "attack" under the *ius in bello*. The key issue here is whether defining these operations as not being attacks can thereby expand the choice of lawful targets beyond the sphere of military objectives. For example, does a denial of service operation against a website constitute an attack? If so, then clearly the categorization of the website attacked as a legitimate military objective—or not—will be a vital concern. But what if denial of service is not an "attack" as understood in LOAC, and how might this affect the legality of directing a cyber operation against the website? In other words, does the nature of the targeted website even matter? Can one engage in cyber operations against non-military targets by claiming that the said cyber operations do not come under the definition of attacks? The *Tallinn Manual*, for example, unequivocally states that the prohibition on attacking civilian objects only applies to cyber operations that qualify as "attacks."[32] These questions are therefore of crucial significance.

The first matter that must be examined in order to answer these questions is whether the principle of distinction is limited only to attacks or whether it covers a wider range of operations. If it is primarily attacks that are covered, then it will be necessary to examine whether cyber operations might constitute attacks as understood in LOAC. Article 48 of Additional Protocol I sets out the following underlying "basic rule": In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives."[33]

This appears to cast a wide net that could include most cyber operations. However, it has been noted by Schmitt that most of the specific rules

---

might have the potential to cross the threshold of international armed conflict." TALLINN MANUAL, *supra* note 21, cmt. to rule 22, ¶ 15.

31. DÖRMANN, *supra* note 18, at 2; Schmitt, *supra* note 30, at 102.

32. TALLINN MANUAL, *supra* note 21, rule 37, cmt. to rule 37, ¶ 2.

33. Additional Protocol I, *supra* note 2, art. 48.

within the relevant section of the Protocol speak not of any operations, but of attacks.[34] There is a debate as to the ways in which the reference to military "operations"—as opposed to a potentially narrower concept of "attack"—provides protection to the civilian population in the cyber context.[35] Notwithstanding that debate, the current analysis focuses on the applicability of the concept of attack to cyber operations because of its paramount importance in the specific rules on targeting and military objectives. In the context of lawful targets, Article 52 states that "[c]ivilian objects shall not be the object of *attack* or of reprisals" and that "[a]*ttacks* shall be limited strictly to military objectives."[36] This too appears to confine the rule to attacks, rather than any operations. This line of reasoning by Schmitt also notes that there are forms of operations, such as psychological operations conducted by militaries, which do not amount to attacks and which may proceed even if targeted at the civilian population.[37]

Article 49 of the Protocol defines "Attacks" as "acts of violence against the adversary, whether in offence or in defence."[38] The reference to violence is also included in the *Commentary* to the Protocol, in relation to the concept of military operations.[39] This leads Schmitt to note the following:

> That Additional Protocol I and its official commentary define both operations and attacks by reference to the notion of violence further strengthens the conclusion that application of the principle of distinction generally depends on an attack having occurred and that an attack is an action during armed conflict that is violent in nature.[40]

Where does this leave cyber operations—might they be considered attacks, and, if not, are they exempt from the principle of distinction, leaving a free choice of targets? One argument, proposed by Dörmann, is that

---

34. Schmitt, *supra* note 30, at 91–93.

35. See the examination of this issue in DINNISS, *supra* note 6, at 196–202.

36. Additional Protocol I, *supra* note 2, art. 52 (emphases added).

37. "[U]nless they cause physical harm or human suffering." Schmitt, *supra* note 30, at 91.

38. Additional Protocol I, *supra* note 2, art. 49(1).

39. "Finally, the word 'operations' should be understood in the context of the whole of the Section; it refers to military operations during which violence is used, and not to ideological, political or religious campaigns." COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 4, ¶ 1875.

40. Schmitt, *supra* note 30, at 93.

> [t]he fact that CNA [computer network attack] does not lead to the destruction of the object attacked is irrelevant. In accordance with Art. 52(2) of AP I only those objects, which make an effective contribution to military action and whose total or partial destruction, capture or neutralization offers a definite military advantage, may be attacked. By referring not only to destruction or capture of the object but also to its neutralization the definition implies that it is irrelevant whether an object is disabled through destruction or in any other way.[41]

But this approach has been countered by Schmitt, noting that the definition of military objectives, from which the neutralization possibility is taken, applies in the context of an attack, and if the cyber operation is not an "attack" as understood in the *ius in bello* then there is actually no need to reach for the military objective definition at all.[42] Although according to this view the requirement for a violent component would rule out certain cyber operations, it would not exclude them all. For an act to be violent in this context, it does not necessarily require a physically violent means of delivery: "'Violence' merely constituted useful prescriptive shorthand for use in rules designed to shield the population from harmful effects. Despite being styled as act-based norms (violence), they are in fact consequence-based."[43] Indeed certain cyber operations—such as in the earlier mentioned examples of taking over missile control systems or dams—can lead to violent effects, and there should be no doubt as to the inclusion of such operations in the rules on attacks. However, this position would exclude many other types of cyber operations from the rules on attacks if their effects do not include casualties or physical damage to objects. Otherwise, it is argued, we could end up ruling that any inconvenience to civilians is prohibited.[44] Cyber operations are thereby presented as often more akin to psy-

---

41. DÖRMANN, *supra* note 18, at 6.

42. Schmitt, *supra* note 30, at 95–96.

43. *Id.* at 93. The *Tallinn Manual* addresses this point as follows:

> "Acts of violence" should not be understood as limited to activities that release kinetic force. This is well settled in the law of armed conflict. In this regard, note that chemical, biological, or radiological attacks do not usually have a kinetic effect on their designated target, but it is universally agreed that they constitute attacks as a matter of law.

TALLINN MANUAL, *supra* note 21, cmt. to rule 30, ¶ 3 (citing Prosecutor v. Tadić, Case No. IT-94-1-l, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶¶ 120, 124 (Int'l Crim. Trib. for the former Yugoslavia Oct. 2, 1995)). *See also Nuclear Weapons, supra* note 4.

44. State practice provides no support for the notion that causation of inconvenience is intended to be prohibited in [international humanitarian law]. On the contra-

chological operations that do not have violent effects, and which would then be permissible even when directed at the civilian networks.[45]

In principle, this analysis is sound and on solid ground. Clearly there are some cyber operations with effects that are equal to any other attack and must therefore be conducted within the LOAC rules on lawful targets. It is equally evident that there may be cyber operations that have no real harmful effect even if directed at civilian networks. There is however, room for significant debate as to where the dividing line lies between these two descriptions and what is the threshold of harm that leads us into the former, requiring adherence to the principle of distinction in choosing targets. In particular, there is a question over the use of physical harm as the threshold.

First, however, a note of caution is perhaps warranted with regard to the analogy between cyber operations and psychological operations, such as disseminating propaganda. The latter operations might be directed at the civilian population by, for example, issuing calls attempting to convince them to abandon support for their leadership:

> The mission of PSYOP is to influence the behavior of foreign target audiences (TAs) to support U.S. national objectives. PSYOP accomplish this by conveying selected information and/or advising on actions that influence the emotions, motives, objective reasoning, and ultimately the behavior of foreign audiences.[46]

Such operations are not considered to be ones that cause direct harm to the civilian population and, as such, can be excluded from certain restrictions placed on attacks.[47] They are therefore a very useful demonstration of how certain types of operations might target the civilian population and remain lawful. But it is less clear that they are the most adequate analogy for cyber operations. The nature of such psychological operations is to convince rather than to create pressure through harm, other than perhaps lowering morale. Cyber operations are, in contradistinction, more often designed

---

> ry, inconvenience and interference with the daily lives of civilians are a frequent result of armed conflict and psychological operations directed against the civilian population are common.

Schmitt, *supra* note 30, at 95.

45. *Id.* at 92.

46. Headquarters, Department of the Army, FM 3-05.30, MCRP 3-40.6, Psychological Operations (2005), *available at* http://www.fas.org/irp/doddir/army/fm3-05-30.pdf.

47. TALLINN MANUAL, *supra* note 21, cmt. to rule 31, ¶ 5 and associated footnotes.

with some form of harmful effect in mind (including relatively low levels of harm, such as denial of service operations to disable a website), even if not always measurable in casualties. There is a difference between morale and harm. Outside of propaganda, what type of analogy might we make with cyber operations directed at civilian networks? If they are designed to change the behavior of the civilian population through adverse pressure, then anything that actively targets civilian networks will likely be causing some type of harm, which may cause it to cross the threshold into what we consider attacks. Other types of operations directed at civilian networks will need to be examined individually and their expected effects must be assessed before making any determination. In other words, it is not that cyber operations are akin to psychological operations because of the cyber format; rather, it is that some specific cyber operations are analogous because their method and produced effect are no more harmful than psychological propaganda operations (for example, during the Russia-Georgia conflict Georgian websites were defaced and made to portray images of President Saakashvili together with a range of dictators).[48] This type of cyber operation has been described as follows: "Another use of cyber war is to send propaganda out to demoralize the enemy, distributing emails and other Internet media in place of the former practice of dropping pamphlets."[49] But this is not true of all cyber operations; therefore a general analogy between cyber operations and psychological ones is too sweeping a generalization that risks minimizing the need to examine the effects of the cyber operations.

III. THE THRESHOLD OF HARM

What then is the threshold of harm that would lead cyber operations to be categorized as attacks subject to the LOAC principle of distinction? There appears to be wide agreement that cyber operations that result in casualties or physical property damage may be categorized as attacks.[50] There is, however, strong reason to question whether physical damage is the most appropriate threshold. Even if such an approach adheres to a stricter reading of the violence requirement, it should be noted that the concept of vio-

48. *See* TIKK, KASKA & VIHUL, *supra* note 7, at 71.

49. CLARKE & KNAKE, *supra* note 6, at 11. The authors also describe the case of the U.S. military sending e-mails to Iraqi officers prior to the U.S. invasion, urging them to abandon their posts and equipment, which many then duly did. *Id.* at 9–10.

50. TALLINN MANUAL, *supra* note 21, rule 30, cmt. to rule 30.

lence is not only physical, but can, for example, include mental suffering.[51] This is well documented in other areas, such as the prohibition of torture, where a wide range of non-physical actions are said to cross the boundary into prohibited torture and ill-treatment due to their severe adverse mental effects.[52] Of course, this is not presented here in order to argue that all cyber operations would fall within this area; it is hardly the case that cutting off the civilian population from their e-mail access would cause mental distress at the level of ill-treatment (although that might be true for some of us). Nevertheless, it serves to demonstrate that when looking at the possible violent effects of a cyber operation in order to ascertain whether it should be considered an attack, we do need to look wider than physical casualties and destruction. In other words, the dividing line is neither the format of the attack nor the physical violence involved, but rather the level of harm caused. It must be stressed at this point that the argument here is not that absolutely any harm would render an operation as being within the definition of attacks. It is clear that there is a threshold that must be crossed, but there is good reason to question whether physical damage is the only possible test for crossing the threshold.

We return, therefore, to the questions surrounding the qualification of cyber operations as attacks—or not—on the basis of their effects. An interesting debate in this regard has emerged through the process surrounding the drafting of the *Tallinn Manual*. There appears to be an emerging view among experts that one of the defining criteria could be the level of effect on the functionality of the targeted object. According to this approach, if the functionality is impaired to the point that it requires replacement of physical components, then this would constitute damage as envis-

51. "While the notion of attack extends to injuries and death caused to individuals, it is, in light of the law of armed conflict's underlying humanitarian purposes, reasonable to extend the definition to serious illness and severe mental suffering that are tantamount to injury." *Id.*, cmt. to rule 30, ¶ 8.

52. This can include mock executions, threats of physical violence, exploitation of the phobias of detainees, and more. The prohibition on causing serious mental suffering or psychological violence has been affirmed in a number of cases at the European, Inter-American and UN human rights bodies, as well as the International Criminal Tribunal for the former Yugoslavia. See analysis and cases cited in NIGEL S. RODLEY & MATT POLLARD, THE TREATMENT OF PRISONERS UNDER INTERNATIONAL LAW 140–43 (3d ed. 2009).

aged in the concept of attack.[53] This approach is not so much a compromise between the earlier mentioned views, but more of a fine-tuning of the idea that for an operation to be an attack, it must cause casualties or damage—and in this case allowing for functionality to be a test for damage or property destruction. If the test still requires there to be physical components that must be replaced, then it ultimately remains very much tied in to the notion of physical property damage.

This insistence on remaining focused on physical property is, however, a position that may require rethinking. A functionality test that requires physical effects would include as an attack a cyber operation that damages a computer system that can be repaired in under an hour by replacing one part, but it would exclude a cyber operation that incapacitates a whole system for two days if there is no physical damage or repair other than waiting for the operation to be over. Moreover, consider this: insisting on physical damage means that blocking enemy communications by physically sabotaging the lines or bombing the telephone or fiber-optic cables would be an attack, but blocking the same communications through cyber operations causing data corruption that does not physically damage property or require replacement of parts is not an attack. What is the basis for this differentiation? The objective sought, the military advantage gained and the effects of the operations will be almost identical. Surely it is not because one requires physically repositioning a telephone pole and the other does not? This seems like an arbitrary distinction that does not take account of modern reality.

This issue is also linked to another question which we face when looking at the definition of military objectives, as it appears in the first Additional Protocol:

> Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.[54]

---

53. TALLINN MANUAL, *supra* note 21, rule 30, cmt. to rule 30, ¶ 10. There was also a subgroup of experts who held the view that this should include loss of functionality that can be restored through reinstalling an operating system.

54. Additional Protocol I, *supra* note 2, art. 52(2).

The problem that arises, which is relatively unique to cyber operations, is whether data can be considered an object. While there is no definitive answer to this question, the currently prevailing view among LOAC experts appears to hold that in most cases data, for the purposes of LOAC targeting, should not be considered an object.[55] This reasoning is said to be supported by well-established interpretations of LOAC, as found in the International Committee of the Red Cross's *Commentary* to the Protocol.[56] According to this *Commentary*, the term "object" refers to something which is "visible and tangible."[57] This, *prima facie*, certainly does not seem to include data. But there is good reason to consider this issue further, and raise the possibility that data may nevertheless be akin to an object in this context. The reference to "visible and tangible" is not part of the Protocol definition, but rather the understanding given to it at a particular point in time and in a specific context. These must be examined more closely to see whether the same reasoning applies to our current situation. At the time of drafting it is unlikely that the drafters would have considered the possibility of data destruction separate from physical damage. Destroying data at the time would have meant physically damaging the storage method, such as the paper files. Today, however, it is perfectly possible to destroy vast quantities of vital data without physically destroying the computers on which they are stored. To place this in context, it raises the question whether a kinetic attack that results in the setting on fire of five hundred mailbags is any more harmful than a cyber operation that permanently deletes five million e-mails. This is a scenario that could hardly have been contemplated when the *Commentary* made the reference to objects being "visible and tangible." Looking beyond this specific phrase into the explanation surrounding its use further reveals why it might not exclude data. While the phrase "visible and tangible" is used to discuss what was being included, it is equally important to see what it was that was being excluded. In fact, the reference to tangible objects is made in order to distinguish ob-

55. "The majority of the International Group of Experts agreed that the law of armed conflict notion of object should not be interpreted as including data." TALLINN MANUAL, *supra* note 21, cmt. to rule 38, ¶ 5. Relatively uncontroversial exceptions include cases where the attack on data leads to casualties or physical damage—in which case it can be said that the object of attack was that which was ultimately harmed. *See id.*, cmt. to rule 30, ¶ 6. Schmitt recognizes certain exceptions, but argues that "[g]enerally, data should not be characterized as an object in itself." Schmitt, *supra* note 30, at 96.

56. TALLINN MANUAL, *supra* note 21, cmt. to rule 38, ¶ 5.

57. "It is clear that in both English and French the word means something that is visible and tangible." COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 4, ¶ 2008.

jects from the very different concept of "general objective (in the sense of aim or purpose) of a military operation."[58] Consequently, it is, therefore, at least arguable that computer data is closer to what the drafters wanted to include as objects than to the notion of what they wanted to exclude as aim or purpose. Indeed, domestic legal systems have demonstrated the ability to evolve beyond physical conceptions of damage to recognize that, rather than physical damage to a computer system, the focus should be on the harm to the contents of the system—data included.[59]

The question of destroying data raises a further matter, the relevance of existing backup data. It might be argued that one of the reasons to exclude data from the rules on attacks is that damage has not occurred if the data can be retrieved. First, however, it should be noted that if this is the argument against viewing data as an object, it does, in fact, allow for *irretrievable* data to be classified as within the rules on attacks. Second, one may question whether potential restoration capability is the correct test for determining the nature of the object and the lawfulness of targeting it. This is not the test we use for physical property. In fact, most physical property is not irretrievable—buildings can be rebuilt, cars can be remanufactured; it is often just a question of cost. Restoration of complex digital data might be restorable from a backup, but this too has a cost. Why is causing one costly act more lawful than the other, and is it just a question of the degree of time and money involved? Perhaps the key here is that data can be backed up so that there are multiple copies, in which case it might be claimed that destroying one copy is not really harmful or damaging since copies exist elsewhere. But how is the attacker to know this? If this is the argument, would the rules on taking precautions require verification of the existence of backup copies?[60] Moreover, once again it is useful to compare this sce-

58. *Id.*, ¶ 2010. See a similar analysis by Dinniss of what the commentators meant to exclude, leading her to note that "any computer program, database, system or virtual network would still be a legitimate target if it meets the above definition, regardless of whether it has a tangible component or exists purely as lines of code." DINNISS, *supra* note 6, at 185.

59. This is evident from the wording of the Computer Misuse Act, 1990, c. 18 (Eng.) and the Police and Justice Act, 2006, c. 48 (Eng.). *See also* R. v. Victor Lindesay, [2001] EWCA (Crim) 1720; R. v. Simon Lee Vallor, [2003] EWCA (Crim) 2288; Regina v. Steven Parr-Moore, [2002] EWCA (Crim) 1907.

60. Additional Protocol I, *supra* note 2, art. 57. Note that this creates an additional problem, since if this argument claims that data destruction is not an attack, one might then say that the rules on precautions in attack do not apply, which would in turn leave us without the rules on verification.

nario to a non-data situation: if a paper document facility or a library is destroyed, do we say it was not an attack because there are copies of the same books in another facility or library? Why treat computer data differently?

Notwithstanding the above, this argument will take on a different shape in the context of cultural objects. It is possible that digital archives might be considered cultural property,[61] and as such benefit from added protections to objects of this type.[62] In this context, backup copies may well play a role, since the uniqueness of an object will often be one of the reasons behind its cultural property protection. If, therefore, it is verifiable and known that additional and equal copies exist and that they will remain unharmed, it may be that a digital item might not benefit from the special protection.[63] But the relevance of backup copies is considered here only in the context of the applicability of extra protections for unique items of cultural value; the general rules on attacking objects should not—as demonstrated above—be affected by this.

There are, of course, limits to the analogies that can be made between the cyber sphere and the physical world. For example, just as we hold discussions of data as objects, some might also question whether computer network systems are considered to be part of the infrastructure of a State; this in turn may lead to a claim that taking over the network infrastructure of a State is akin to taking over its territory.[64] Considering that we have already seen arguments being made in the context of Gaza that a State should be considered an occupying power due to control exerted from the outside and without boots on the ground,[65] might we one day see arguments calling for the obligations stemming from the laws of occupation to be applied to occupation through control of network infrastructure? This

---

61. See examples in the TALLINN MANUAL, *supra* note 21, cmt. to rule 82, ¶ 5.

62. Convention for the Protection of Cultural Property in the Event of Armed Conflict, May 14, 1954, 249 U.N.T.S. 240; Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict art. 22, Mar. 26, 1999, 2253 U.N.T.S. 212.

63. See discussion in TALLINN MANUAL, *supra* note 21, cmt. to rule 82, ¶ 6.

64. *But see id.*, ch. VI, ¶ 3 ("[C]yber operations cannot alone suffice to establish or maintain the degree of authority over territory necessary to constitute an occupation.").

65. The debate over the status of Gaza contains some genuinely complex questions as to the definition, nature and purpose of the laws of occupation. For an examination of some of these issues, see, e.g., Yuval Shany, *Faraway, So Close: The Legal Status of Gaza after Israel's Disengagement*, 8 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 2005, at 369–83 (2005). See also the opinions expressed in SARI BASHI & KENNETH MANN, DISENGAGED OCCUPIERS: THE LEGAL STATUS OF GAZA (2007), a*vailable at* http://www.gisha.org/UserFiles/File/Report%20for%20the%20website.pdf.

sounds extremely far-fetched, and probably rightly so. As the *Tallinn Manual* correctly points out, "[t]here is no legal notion of occupation in cyberspace."[66] The creation of such a notion is *not* an argument being proposed or supported here; its possibility is simply being raised as a warning sign of things to come.

However, just as the attempts to apply the law to cyber realities might be stretched beyond credibility, equally, attempts to resist updated interpretations will result in stagnant and even obsolete rules. To avoid both misapplication and obsolescence, we must accept that the law cannot forever be interpreted and applied in exactly the same manner, lock, stock and barrel. If we wish to ensure the relevance of the rules to the twenty-first century, it is vital that they are interpreted in light of modern reality. Proposing new interpretations is not the same as saying the law itself is inadequate to deal with new challenges. While there are times that new laws are deemed necessary to confront contemporary battlefield realities,[67] at other times we may be able to rely on the existing body of international law for many of the current and future challenges, just as its general principles have been deemed applicable to numerous technological advances during the past century:

> Indeed, nuclear weapons were invented after most of the principles and rules of humanitarian law applicable in armed conflict had already come into existence; the Conferences of 1949 and 1974–1977 left these weapons aside, and there is a qualitative as well as quantitative difference between nuclear weapons and all conventional arms. However, it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all

66. TALLINN MANUAL, *supra* note 21, ch. VI, ¶ 3.

67. A clear example of these is the adoption of the 1977 Additional Protocols to the 1949 Geneva Conventions, which contained rules designed to cover developments on the battlefield in relation to means, methods and participants in combat. *See also Nuclear Weapons*, *supra* note 4, ¶ 76 ("Since the turn of the century, the appearance of new means of combat has—without calling into question the longstanding principles and rules of international law—rendered necessary some specific prohibitions of the use of certain weapons, such as explosive projectiles under 400 grammes, dum-dum bullets and asphyxiating gases. Chemical and bacteriological weapons were then prohibited by the 1925 Geneva Protocol.").

> kinds of weapons, those of the past, those of the present and those of the future.[68]

There should be no doubt that existing law can apply to the cyber sphere, but there must be room for new approaches and interpretations that might differ from the manner in which the same law was read in the past.[69] The earlier discussion of considering data as an object for the purpose of targeting rules is a case in point. The law itself does not exclude the possibility; rather, those who exclude data do so by relying on past interpretations of the law that were necessarily wedded to the time.[70] Instead, it is perfectly possible to remain true to the object and purpose of the law—and indeed to the letter of the law itself—by interpreting it in light of the modern-day context in which it is being implemented.[71] This is therefore a call for new interpretations in light of reality, and not a call to overhaul the law itself.[72] In the context of cyber operations, this requires rethinking the nature of harm required for crossing the threshold into actions that are regulated by the rules on attacks. Rather than focus on the *type* of harm, the focus should be on the *level* of harm, regardless of whether or not the effects are caused through physical destruction. Massive deletion of data from institutional archives (e.g., educational institutions, local councils, government offices) is an example of an act which can cause a significant

---

68. *Id.*, ¶ 86.

69. See, for example, the White House International Strategy for Cyberspace:

> The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them.

THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

70. *See, e.g.*, referring to objects as "visible and tangible." *See supra* text accompanying note 57.

71. The first rule on the interpretation of treaties states that "[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty *in their context* and *in the light of its object and purpose*." Vienna Convention on the Law of Treaties art. 31.1, May 23, 1969, 1155 U.N.T.S. 331 (emphasis added).

72. There are, however, also arguments being made for creating new laws to regulate cyber operations. See, e.g., the call for a new framework of "international law for information operations" in Duncan B. Hollis, *Why States Need an International Law for Information Technology*, 11 LEWIS & CLARK LAW REVIEW 1023 (2007).

level of harm without leading to physical destruction or casualties. These should at the least be considered as having crossed the threshold so as to be regulated by the rules on attacks, and subject to the principle of distinction with regard to choice of targets.

The above questions on the categorization of operations as attacks must also be viewed in light of the underlying concerns behind some of the positions. Much of this debate is occurring in the context of excluding certain operations from the definition of attacks so that they will not be hampered by the restrictions placed in LOAC, and so that we do not end up describing any disruption to civilian networks as unlawful.[73] But this concern is, to a certain extent, misplaced. Note that we are seeking to examine the categorization of operations *directed* against civilian networks, and *not* about operations against so-called dual-use networks.[74] *Directing* operations against civilian networks *intending* to cause negative effects for the civilian population should not be an encouraged military activity, and by ensuring that these operations are considered attacks, we can afford better protection to civilians. At the same time, having a lower threshold of toleration for operations against pure civilian networks should not have a detrimental effect on military needs—it does *not* prevent attacks on dual-use networks, which could be legitimate military objectives.[75] If the primary concern is the latter, then this debate is misplaced since defining the operation as an attack would still allow for the target to be a legitimate military objective. The primary concern would then be the separate matter of indiscriminate attacks or collateral damage, and whether the harm caused to the civilians is acceptable disruption or rises to the level of damage that tips the balance in the proportionality formula—but these are separate questions from our current focus on the lawfulness of choosing a particular target.[76]

A final point on whether cyber operations are "attacks" is a reminder that in other contexts States have rightly clarified that when analyzing the legality of an attack, one must look at the attack as a whole,[77] recognizing

---

73. Schmitt, *supra* note 30, at 95.

74. Note that under LOAC there is no specific rule for categorizing objects as dual-use. They are either a military objective or not. The fact that a military objective may be used for civilian purposes does not remove its status as a military objective, but will have consequences with regard to the precautions, and means and methods employed, which can then in turn determine the lawfulness of the attack.

75. Schmitt, *supra* note 30, at 96.

76. For issues relating to how an attack may be carried out, see *supra* note 18.

77. For example, see the statement of the United Kingdom on Articles 51 and 57 upon ratification of Additional Protocol I that "the military advantage anticipated from an

that a specific operation might be "part of the complex mosaic of a bigger integrated operation."[78] To apply this to the question at hand, if a cyber operation that alone might not have been described as an attack is, in fact, an inherent component in a collection of operations that form a single attack, then this cyber operation must be assessed within the laws applicable to attacks,[79] including the question of its target. For example, disabling a communications network for a few hours might not seem to cause serious harm, but if this is carried out in order to mask other activity that enables a devastating attack to occur while the enemy cannot communicate then clearly the cyber operation was part of the attack.[80] Again, as noted in the previous point, this does not place undue restrictions on the cyber operation if its target is indeed a military communications system.

Notwithstanding all the above, and while it has been argued above that there is a need to reconsider the threshold of harm in light of the potential for serious non-physical harm, by definition having a threshold means that there will be a possibility for certain circumstances to remain below it. Accordingly, there will be certain cyber operations that do not reach the required threshold (e.g., cyber operations that are propaganda/psychological operations) and which would not constitute an "attack" as defined in the law. If so, then the law of armed conflict might not prohibit such an operation even if directed at a civilian network. We should, however, remember that the law of armed conflict is far from being the only legal framework in existence. Such operations would not take place in a legal black hole; indeed, much attention has been given in recent years to the risks created by claiming legal vacuums.[81] Depending on the precise circumstances, a host of other laws might apply, ranging from telecommunication laws,[82] princi-

attack is intended to refer to the advantage anticipated from the attack considered as a whole and not only from isolated or particular parts of the attack." International Committee of the Red Cross, Reservation/Declaration Text, http://www.icrc.org/ihl.nsf/NORM/0A9E03F0F2EE757CC1256402003FB6D2?OpenDocument%20 (last visited Nov. 19, 2012).

78. Stefan Oeter, *Methods and Means of Combat*, *in* THE HANDBOOK OF HUMANITARIAN LAW IN ARMED CONFLICTS 105, 162 (Dieter Fleck ed., 1995).

79. TALLINN MANUAL, *supra* note 21, cmt. to rule 30, ¶ 16.

80. For an example of combining cyber operations as an element leading to physical attack, see the description of the Israeli attack on the Syrian alleged nuclear facility in CLARKE & KNAKE, *supra* note 6, at 1–8.

81. Most notably in the debates surrounding the applicability of international humanitarian law and human rights law to actions taken in the "war on terror."

82. International Telecommunication Convention, Nov. 6, 1982, S. TREATY DOC. NO. 6, 99th Cong., 1st Sess. (1985); Optional Protocol on the Compulsory Settlement of

ples of non-intervention,[83] outer space treaties[84] and human rights law[85] to domestic criminal law or international agreements on cyber crime.[86] The applicability of these branches of law will vary from case to case based on the precise circumstances, and they may themselves be subject to debate (an obvious example of debate is the disagreement over extraterritorial applicability of international human rights law).[87] However, they cannot be ignored and their applicability must at least be considered. This is, in fact, not only the case when LOAC does not apply to the operations; indeed, some of these branches of law may well apply also during armed conflict, though once again this will depend on the specific branch of law under discussion, and the interplay between it and LOAC will need to be taken into account.[88]

Disputes Relating to the Constitution of the International Telecommunication Union, to the Convention of the International Telecommunication Union and to the Administrative Regulations, Dec. 22, 1992, S. TREATY DOC. NO. 104-34, 104th Cong., 2nd Sess. (1996).

83. For example, under the Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, G.A. Res. 2625, Annex, U.N. GAOR, 25th Sess., Supp. No. 28, U.N. Doc. A/8028, at 121 (Oct. 24, 1970).

84. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 610 U.N.T.S. 205. See discussion of applicability of outer space treaties in James P. Terry, *The Lawfulness of Attacking Computer Networks in Armed Conflict and in Self-Defense in Periods Short of Armed Conflict: What Are the Targeting Constraints?*, 169 MILITARY LAW REVIEW 70, 87–88 (2001).

85. International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), U.N. Doc. A/6316 (Dec. 16, 1966), 999 U.N.T.S. 171; International Covenant on Economic, Social and Cultural Rights, G.A. Res. 2200A (XXI), U.N. Doc. A/6316 (Dec. 16, 1966), 993 U.N.T.S. 3.

86. Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185.

87. LUBELL, *supra* note 22, ch. 8.

88. The interplay between the law of armed conflict and international human rights law has been subjected to extensive scrutiny, albeit not yet resolved. *See, e.g.*, Cordula Droege, *The Interplay Between International Humanitarian Law and International Human Rights Law in Situations of Armed Conflict*, 40 ISRAEL LAW REVIEW 310 (2007); Nancie Prud'homme, Lex Specialis: *Oversimplifying a More Complex and Multifaceted Relationship?,* 40 ISRAEL LAW REVIEW 356 (2007); Françoise J. Hampson, *Is Human Rights Law of Any Relevance to Military Operations in Afghanistan?*, *in* THE WAR IN AFGHANISTAN: A LEGAL ANALYSIS 485 (Michael N. Schmitt ed., 2009) (Vol. 85, U.S. Naval War College International Law Studies); Noam Lubell, *Challenges in Applying Human Rights Law to Armed Conflict*, 87 INTERNATIONAL REVIEW OF THE RED CROSS 737 (2005); U.N. Econ. & Soc. Council, Comm'n on Human Rights, Subcomm. on the Promotion & Protection of Human Rights, Françoise J. Hampson & Ibrahim Salama, *Administration of Justice, Rule of Law and Democracy:*

IV. CONCLUSION

Cyber operations taking place during armed conflict can present a number of challenges in discerning the correct legal framework for their regulation. Notably, they are an awkward fit for the rubric of laws relating to attacks, as these were clearly designed with the primary focus on kinetic attacks. In particular, there is the possibility that excluding cyber operations from the notion of attack would thereby release these operations from the requirement to adhere to the principle of distinction in the choice of targets—one of the fundamental principles at the heart of the law of armed conflict. Clearly, cyber operations that lead to direct physical damage or casualties must be considered attacks. Likewise, those cyber operations that amount to no more than propaganda and cause no actual harm might lie outside the notion of attacks. This article has argued, however, that the dividing line between these two poles cannot rely on the physical nature of the harm caused. Rather, the key criteria for the threshold at which an operation must be regarded as an attack under the law of armed conflict must rest on the level of harm caused, and this can include non-physical damage. Such an understanding does not require new laws, but can be a legitimate interpretation of the current law, in line with both its object and purpose, and a better reflection of modern reality.

Working Paper on the Relationship Between Human Rights Law and International Humanitarian Law, 57th Sess., U.N. Doc. E/CN.4/Sub.2/2005/14 (June 21, 2005).

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference

Yoram Dinstein

89 INT'L L. STUD. 276 (2013)

Volume 89 2013

Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference

Yoram Dinstein[*]

I. INTRODUCTION

Truth to tell, I am more than a little bothered and bewildered by the direction taken in a considerable portion of the papers submitted to the conference and in the deliberations that ensued.

Why bewildered? The problem may be semantic, but when I was invited to participate in a conference on "cyber war," I fully expected—as a layperson in the cyber sphere of activities—to encounter difficulties in decoding a specialized experts' jargon with which I am not closely acquainted. Indeed, when the first speaker mentioned clouds, I thought that he was talking about inclement weather. When another participant talked about malware, it sounded to me like a reference to a breach of the dress code. What really surprised me, however, was that so many participants—while displaying the most intimate familiarity with the "cyber" vocabulary—were apparently stymied by the concept of "war."

I should have thought that, for the military at least, the expression, "war," is largely a no-brainer. Should it not have been self-evident to every person present that war postulates an armed conflict? Yet, panelist after panelist—even among those associated with United States Cyber Com-

* Professor Emeritus, Tel Aviv University, Israel.

mand—addressed issues that pertain in a generic manner to illicit cyber operations (of heterogeneous characterizations and motivations) having no apparent linkage to an ongoing or prospective war.

This bothers me. Having been twice the victim of "phishing" expeditions into my e-mail account, I am acutely interested in what can be done to stop peacetime intrusions into somebody else's private cyber domain. I am fascinated by the entire range of problems extending from "hacking" to grand-scale theft of intellectual property in peacetime. Nevertheless, surely, this is not why this conference was convened at the Naval War College. Our remit was "cyber war," and this is what ought to have attracted our attention—to the exclusion of any diversionary items on anybody's pet agenda.

As an illustration of the disorientation stoked by the departure from the straight–and–narrow meaning of "cyber war," let me point at the rather prolonged verbal give–and–take that went on in connection with the theme of sovereignty. I freely concede that sovereignty is a topic that ought to be of interest to anyone interested in international law. I have myself written about it,[1] and I find the evolution of this centuries-old precept to be of compelling import. All the same, I do not propose to go into the intricacies of the matter. I would have liked to critique at length some of the peculiar notions of sovereignty advanced in this conference. I shall not succumb to the temptation for the plain reason that the subject is largely irrelevant to cyber warfare.

It must be acknowledged that the sovereignty of enemy countries in wartime is trampled underfoot without the slightest hesitation. Thus, when the United States launched its devastating "shock and awe" attack on Baghdad in 1991, did anyone in the Department of Defense spend even five seconds mulling over Iraqi sovereignty? The question is rhetorical. And, if enemy sovereignty can be totally ignored in kinetic warfare, why should it be of greater weight when cyber warfare comes into the picture? There is one salient case in which sovereignty in wartime retains its full vigor, and that is neutrality: the sovereignty of neutral States must be fully deferred to by all belligerent parties. But that is a side issue when compared to the mortal blows that the antagonists deal to each other.

What the conference ought to have concentrated on is how cyber operations bring about or are prosecuted in war. This was properly done by a

1. *See* Yoram Dinstein, *Sovereignty, the Security Council and the Use of Force*, *in* REDEFINING SOVEREIGNTY: THE USE OF FORCE AFTER THE COLD WAR 111, 111–22 (Michael Bothe, Mary Ellen O'Connell & Natalino Ronzitti eds., 2005).

number of lecturers. I shall devote my remarks to the highlights of their presentations, adding a few points of my own.

In the framework of war, cyber operations invite analysis from the respective standpoints of both the *jus ad bellum* and the *jus in bello*.

II. THE *JUS AD BELLUM*

As far as the *jus ad bellum* is concerned, the cardinal question is not (as suggested repeatedly) whether a cyber operation rises to the level of use of force, but whether it reaches the threshold of an armed attack. The use of inter-State force is strictly forbidden in Article 2(4) of the United Nations Charter,[2] as well as in customary international law.[3] But, unless that use of force qualifies as an armed attack—pursuant to Article 51 of the United Nations Charter[4] and customary international law,[5] which lay the ground for the exercise of the right of self-defense—the response of the target State is necessarily limited in scope. As long as the use of force does not amount to an armed attack, the target State can bring the matter before the Security Council, it can employ non-forcible countermeasures or it can sue (assuming that some international court or tribunal is vested with jurisdiction). But it cannot use counterforce in self-defense.

There is a vital fork in the road facing the State that has fallen victim to an unlawful use of force. In the musical *Guys and Dolls*, the famous lyrics are: "Sue me, sue me / Shoot bullets through me." Still, as anyone who is not in the musical business will readily perceive, there is a critical discrepancy between the options of "Sue me, sue me" and "Shoot bullets through me." Consistent with Article 51, shooting bullets (as distinct from reliance on litigation), in response to the use of force, is permissible only when an armed attack occurs. I do not want to go into the thorny issue of anticipatory self-defense. Suffice it to say that I do not subscribe to the notion that anticipatory self-defense (preceding an expected armed attack) is compatible with Article 51. At the same time, I propound the legality of

2. Charter of the United Nations, June 26, 1945, *reprinted in* 9 INTERNATIONAL LEGISLATION: A COLLECTION OF THE TEXTS OF MULTIPARTITE INTERNATIONAL INSTRUMENTS OF GENERAL INTEREST 327, 332 (Manley O. Hudson ed., 1950).

3. *See* Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 99–100 (June 27) [hereinafter *Nicaragua*].

4. Charter of the United Nations, *supra* note 2, at 346.

5. *See Nicaragua*, *supra* note 3, at 94.

interceptive self-defense in reaction to an embryonic armed attack which has already commenced.[6]

A query posed by multiple interlocutors—from the dais as much as from the floor—is whether there exists a gap between Article 2(4) (use of force) and Article 51 (armed attack). My answer is definitely affirmative. I put it to you that it would defy logic to maintain that, in one of the most carefully crafted instruments in the history of international law (the Charter of the United Nations, serving as a semi-constitution of the contemporary international community), the framers resorted to divergent phraseology—"use of force," on the one hand, and "armed attack," on the other—to describe exactly the same phenomenon.

As we have been given to understand, the United States government apparently does not recognize the gap between Article 2(4) and Article 51. But, if so, this would be no more than a knee-jerk reaction to the fact that the gap was overemphasized in the *Nicaragua* judgment of 1986[7] (which the United States has many justifiable grounds to resent). I do not deny that in *Nicaragua* the International Court of Justice went too far in its assessment of the dimensions of the gap. Preeminently, the Court did not view "a mere frontier incident" as an armed attack.[8] I find this to be an untenable position. It was carried to its illogical conclusion by the Eritrea-Ethiopia Claims Commission's incongruous holding of 2005, whereby border clashes between infantry units, even when leading to bloodshed, do not make the grade of an armed attack.[9]

In my opinion, the gap between Article 2(4) and Article 51—while there—must be seen in its right proportions. What the gap denotes is that a use of force not involving loss of life or significant destruction of property falls short of an armed attack.[10] If a soldier of State *A* shoots across the border of State *B*, killing a cow, this is an instance of use of force. But, absent a minimal degree of gravity, the act (albeit unlawful) does not rank as an armed attack. An armed attack must leave behind a trail of human casualties or ample destruction of property. Only when that happens is it justi-

---

6. *See* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 203–5 (5th ed. 2011).

7. *See Nicaragua*, *supra* note 3, at 101, 110.

8. *Id.* at 103.

9. Eritrea-Ethiopia Claims Commission, Partial Award, *Jus ad Bellum* (Ethiopia's Claims 1-8), 2005, 45 INTERNATIONAL LEGAL MATERIALS 430, 433 (2006).

10. *See* DINSTEIN, *supra* note 6, at 208.

fied to have recourse to counterforce while invoking the right of self-defense (as per Article 51).

There is a certain reluctance to admit that cyber attacks—no less than kinetic attacks—may be categorized as armed attacks under Article 51. I cannot explain this attitude. Laypeople may be misguided by the invisibility of the electrons set in motion by a cyber attack. Contrarily, cyber experts may be so captivated by the act of tampering with the integrity of the target computer that they lose sight of the external lethal/destructive effects of the attack. This would be parallel to artillerists concerned with the design of armor-piercing shells who do not ponder what havoc would happen once the projectiles have penetrated their targets.

In essence, cyber (as has been stressed in sundry presentations) must be looked upon as a new means of warfare—in other words, a weapon: no less and no more than other weapons. As with all known weapons, the test of a new weapon is not how intimidating it looks—or how ingeniously the novel mechanism works—but what harm it is liable to produce.

In its 1996 advisory opinion on the *Legality of the Threat or Use of Nuclear Weapons*, the International Court of Justice underscored that Article 51 does not refer to any specific weapon: the provision applies to (and permits self-defense in response to) all armed attacks, regardless of the weapon employed in pressing the attack.[11]

The same legal scrutiny should take place when the yardsticks are those of customary international law. The legal principles of the customary *jus ad bellum* remain intact whether the armed attack is kinetic or cyber. Self-defense in response to cyber armed attacks can take place under customary international law, as much as under Article 51. It is immaterial that, as yet, no explicit State practice has crystallized concerning the exercise of the right of self-defense against cyber armed attacks.[12] There is no need for State practice to develop separately as regards every concrete weapon employed in an armed attack.

It should be added that, when exercised against a cyber armed attack, self-defense need not be circumscribed to "cyber-on-cyber" warfare. Once a State is at war (in light of the *jus ad bellum*), it can use all the military assets available to it (within the limits of the *jus in bello*), whether they are kinetic or cyber.

---

11. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, 244 (July 8).

12. *See* Marco Roscini, *World Wide Warfare*—Jus ad Bellum *and the Use of Cyber Force*, 14 MAX PLANCK YEARBOOK OF UNITED NATIONS LAW 85, 123–24 (2010).

Already in 1999, at a previous Naval War College conference on computer network attacks (as they were then called), I observed that these attacks can cause fatalities through gaining control of target computers, causing a shutdown of computer–controlled life–support systems, deadly aircraft crashes, ruinous floods (by opening the sluices of high dams) and even the doomsday scenario of the meltdown of a nuclear reactor.[13] A lot has transpired since 1999. What looked at the end of the twentieth century to be a sci-fi fantasy is increasingly becoming a realistic script for the twenty–first century.

III. ATTRIBUTION

No doubt, the attribution of a cyber attack to its real source may be fraught with difficulties. But is this a unique feature of cyber war? In actuality, attribution is often challenging even in circumstances of kinetic warfare, especially at sea. Reference has been made to the famous *Corfu Channel* case of 1949.[14] Well, what were the facts there? In 1946, two British destroyers struck mines laid in Albanian territorial waters, which are part of the Corfu Channel, an international strait between the Greek island of Corfu and the Albanian coast. The explosions caused heavy damage to the destroyers and dozens of casualties among the British sailors. Albania lost the case on the ground that it must have known of the existence of the minefield, and that it should have warned the approaching British warships of the imminent danger within its territorial waters.[15] Yet, interestingly, the International Court of Justice did not find sufficient evidence to establish who exactly had laid the mines (although the spoor led to the door of neighboring Yugoslavia), and pronounced that the origin of the mines remained a matter of conjecture.[16]

It may be added that in 1937—at the time of the Spanish Civil War—an arrangement was concluded in Nyon "against piratical acts by submarines," perpetrated in the Mediterranean by unknown submarines and resulting in the sinking of merchant ships not belonging to the opposing parties.[17] This was an exceptional instrument, which treated activities by

13. Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99, 105 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (Vol. 76, U.S. Naval War College International Law Studies).

14. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 6 (Apr. 9).

15. *Id.* at 22–23.

16. *Id.* at 16–17.

17. Nyon Arrangement, Sept. 14, 1937, 181 L.N.T.S. 135, 137.

submarines—i.e., government warships—as piratical, although as a rule piracy is restricted to acts committed by private persons for private ends.[18] The rationale underlying the Nyon Arrangement was that the submarines in question (suspected to be either German or Italian) could not be identified, and no State assumed responsibility for their depredations.[19]

I do not underrate the imperative need of tracing back a cyber (or a kinetic) attack to its source. It would be reckless (and senseless) to strike back hastily at the ostensible fount of a cyber attack, for the target State (State *B*) may be lashing out at an innocent party (State *C*) in lieu of the culpable actor (State *A*). However, as we were informed by the Cyber Command experts, tracing back the originator of a cyber attack is normally feasible: the catch is that it is time-consuming.

I fail to see the great peril posed by a delay in identifying the State responsible for a cyber attack. After all, if the unattributed cyber attack is an isolated event (not followed by any other attack), there is no inexorable rush to figure out instantaneously who is really behind it. Conversely, if the cyber attack is only the precursor of a stream of other attacks in its wake, source verification is likely to become much easier and faster.

Does the fact that a cyber attack is mounted without disclosure of identity instigate an ethical issue (as has been suggested)? I do not see why there is anything intrinsically wrong (at least legally) in an attacker not showing his hand overtly. In kinetic warfare, a sniper does not disclose his identity or whereabouts. Why should a cyber attacker behave differently?

Patently, the legal dissection undergoes a radical transformation if the cyber attacker does not only strike anonymously but is masquerading behind a specific false front (from which the cyber attack appears to have emanated). It then depends on the character of that fraudulent front. If it is, say, a hospital or a school, the deceitful conduct is no different from the behavior of a kinetic attacker hiding behind or among civilian "human shields."[20] The *jus in bello* strictly forbids the use of "human shields" as a method of warfare.[21]

---

18. See the definition of piracy in Article 101 of the 1982 Law of the Sea Convention. United Nations Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 3.

19. L.F.E. Goldie, *Terrorism, Piracy and the Nyon Agreements*, *in* INTERNATIONAL LAW AT A TIME OF PERPLEXITY: ESSAYS IN HONOUR OF SHABTAI ROSENNE 225, 240–44 (Yoram Dinstein ed., 1989).

20. On "human shields," see YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 152–55 (2d ed. 2010).

21. *See* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 51(7), June 8,

IV. THE *JUS IN BELLO*

Assuming that war is already raging (whether its onset was a cyber or a kinetic armed attack), the *jus in bello*—a.k.a. the law of armed conflict (LOAC) or international humanitarian law—automatically applies. We have been told over and over of the need to apply LOAC to cyber warfare "by analogy." But, to my mind, there is no room in this context for an analogy, which by its nature is based on conceptual similarity and correspondence. There is nothing extraordinary in cyber warfare: it is just ordinary warfare with a little bit of extra. Cyber warfare does not merely resemble other forms of warfare: it is warfare. As such, it is directly governed by the *jus in bello*.

Concerns have been raised about the clarity of the LOAC *lex lata*. I find these concerns both exaggerated and unreal:

(i) These concerns are exaggerated, because (as shown by Herbert Hart) every legal rule includes a nucleus of clarity surrounded by a penumbra of uncertainty, the meaning of which may prove doubtful in certain circumstances.[22] Several panelists dwelt upon the penumbra of LOAC rules. However, the nucleus of the rules is equally there.
(ii) Scholarly doubts about the state of the *lex lata* are unreal, since they are not shared by the end users of LOAC. The armed forces of States constantly reiterate LOAC rules in their military manuals, applying and enforcing them quite rigorously. There is also a modicum of international enforcement today. The Yugoslav Tribunal (the ICTY) has already come up with extensive jurisprudence, which shows that LOAC is alive and kicking as a robust legal system.[23]

In keeping with LOAC, cyber operations do not automatically come within the ambit of the definition of "attacks," which are defined as "acts of violence against the adversary, whether in offence or in defence."[24] The condition of violence is *sine qua non*. Unlike an armed attack under the *jus ad*

1977, 1125 U.N.T.S. 3, *reprinted in* THE LAWS OF ARMED CONFLICTS: A COLLECTION OF CONVENTIONS, RESOLUTIONS AND OTHER DOCUMENTS 711, 736 (Dietrich Schindler & Jiri Toman eds., 4th ed. 2004) [hereinafter Additional Protocol I].

22. H.L.A. HART, THE CONCEPT OF LAW 11–12 (1965).

23. *See, e.g.*, Prosecutor v. Blaškić, Case No. IT-95-14-T, Judgment (Int'l Crim. Trib. for the former Yugoslavia Mar. 3, 2000); Prosecutor v. Blaškić, Case No. IT-95-14-A, Appeal Judgment (Int'l Crim. Trib. for the former Yugoslavia July 29, 2004).

24. Additional Protocol I, *supra* note 21, art. 49(1) at 735.

bellum, a *jus in bello* attack would embrace my previous bovine example: if a cow is killed by enemy fire, that is an attack under LOAC. All that is necessary is death/injury to human beings or more than nominal damage to property. The same acid test is applied to all types of warfare, whether kinetic or cyber. If the consequences of a cyber operation are human death/injury or tangible property damage, it constitutes an attack compatible with LOAC requirements.[25]

Accordingly, a cyber operation does not pass muster as an "attack" if it is limited to (i) intelligence gathering (through collection of data and information); (ii) disruption of communications; or (iii) issuing false orders to enemy forces. I therefore fail to see why the mere planting of a "worm" in an enemy computer (without destroying it) is tantamount to an attack.

As for intelligence gathering, it must be appreciated that espionage per se is not prohibited by LOAC, although the individual spy (engaging in this activity behind enemy lines and out of uniform) may be punished by the enemy if he falls into its hands during such an engagement.[26]

Under the fundamental principle of distinction, attacks—whether cyber or kinetic—must be confined to lawful targets, to wit, combatants, civilians directly participating in hostilities or military objectives. What does this mean in concrete cyber terms?

First and foremost, direct attacks against civilian computers—or other civilian objects—are prohibited. This is the incontestable nucleus of a basic rule of LOAC governing kinetic, as well as cyber, attacks. The penumbra relates to the definition of a civilian computer. The general definition of civilian objects is negative: "all objects which are not military objectives."[27] The same proposition applies also to computers: civilian computers are those that are not military computers.

Like all military objectives, military computers are defined by their "nature, location, purpose or use."[28] A non-exhaustive list of military computers by nature would include (i) computers designed as components in kinetic weapons or weapon systems, e.g., in artillery, tanks, warships, military

25. *See* Michael N. Schmitt, *CNA and the* Jus in Bello*: An Introduction*, *in* PROCEEDINGS OF AN INTERNATIONAL EXPERT CONFERENCE ON COMPUTER NETWORK ATTACKS AND THE APPLICABILITY OF INTERNATIONAL HUMANITARIAN LAW 101, 112 (Karin Byström ed., 2004).

26. On espionage, see HARVARD PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE rules 118–24 (2009).

27. Additional Protocol I, *supra* note 21, art. 52(1) at 737.

28. *Id.*, art. 52(2).

aircraft or missiles; (ii) computers designed to facilitate the logistical operation of military units; and (iii) computers designed for the production or supply of munitions, the development of new weapons, etc.

Run-of-the-mill computers (to wit, those that are not military computers by nature) may become military computers by use simply due to serving combatants for military purposes. This broad classification encompasses not only computers containing sensitive operational data or classified military information. Once computers are used in the discharge of military duties—even if they are dedicated to mundane administrative tasks, such as innocuous and unclassified correspondence—they are military objectives.

In case of doubt whether a computer is civilian or military, it must be viewed as civilian.[29] But this is not as simple as it sounds. For instance, if a civilian uses a computer that previously served a member of the armed forces, the fact that the military software has been removed does not settle the matter inasmuch as the hardware may be contaminated; the hard drive of the computer may still contain unerased military data.

Apart from direct attacks against civilian computers, LOAC interdicts indiscriminate attack. When a malicious destructive "virus" is planted in enemy military computers—absent any control over the possibility of its spreading unchecked to civilian computers—this will be considered an unlawful indiscriminate attack.[30] In terms of being indiscriminate, the act of planting a virtual destructive virus must be deemed to be on a par with that of planting a lethal biological virus.

Empirically, the crux of the issue in cyber as much as in kinetic attacks is proportionality in terms of collateral damage. The general rule is that when lawful targets are attacked, collateral damage to civilians/civilian objects must not be expected to be "excessive" in relation to the "concrete and direct" military advantage anticipated.[31] A cyber attack may in fact cause less collateral damage than a kinetic attack on the same site.[32] But even a cyber attack may trigger a host of civilian casualties and massive destruction to civilian objects. When will the casualties and/or destruction be considered "excessive"? Here the penumbra is more spacious than usual,

29. *Id*., art. 52(3).

30. *See* Johann–Christoph Woltag, *Cyber Warfare*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 988, 991 (Rüdiger Wolfrum ed., 2012).

31. *See* Additional Protocol I, *supra* note 21, art. 51(5)(b) at 736.

32. *See* Herbert S. Lin, *Operational Reality of Cyber Warfare*, *in* INTERNATIONAL HUMANITARIAN LAW AND NEW WEAPON TECHNOLOGIES 137, 140 (Wolff Heintschel von Heinegg ed., 2012).

there being no scientific way to measure when losses and damage are "excessive" compared to the military advantage anticipated. Still, it is taken for granted that the attacker must behave in a reasonable manner.

I have alluded to the need for the military advantage anticipated to be "concrete and direct," that is to say, not just abstract or speculative. However, military advantage has to be looked at in a holistic fashion. When a large-scale attack is in progress, the outlook would be distorted if every discrete segment were assessed in isolation: it is required to put in balance the overall campaign.[33] Ergo, if a cyber attack is launched systematically against an entire array of enemy military computers, with dire consequences for civilians/civilian objects by way of collateral damage, the military advantage must be evaluated from a comprehensive perspective. Parsing the piecemeal benefits accruing from strikes against particular target computers may not tell the story accurately. The whole may be greater than the sum of its parts.

V. A NEW TREATY?

I share the view that there is no point at the present juncture in seeking to initiate a new treaty promulgating a code of conduct in cyber warfare. First, I cannot imagine that States would be ready and willing to undertake anytime soon the arduous process of formulating such a treaty. But, second, I do not think that the projected treaty (if it were to be drafted) would do more than enunciate the general norms of LOAC.

Bear in mind that this is by no means the first time in the history of LOAC that the introduction of a new weapon has created the misleading impression that great legal transmutations are afoot. Let me remind you of what happened upon the introduction of another new weapon, *viz.*, the submarine. The full potency of that weapon came to light in World War I, when the unrestricted U-boat offensive almost choked the Allied countries. In the postwar era, many voices were raised in favor of adopting a new general treaty coming to grips with this controversial innovation. What was the outcome? After two failed attempts and much soul-searching, a *procès-verbal* was successfully concluded in London in 1936. Yet, all that the authors of the *procès-verbal* managed to accomplish was proclaiming that "submarines must conform to the rules of international law to which sur-

33. *See* UNITED KINGDOM MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 5.4.4 (2005).

face vessels are subject" (accentuating some particulars).[34] I am positive that, if a treaty on cyber warfare were done today, it would similarly stipulate in an anodyne fashion that the general rules of LOAC must be conformed with.

VI. CONCLUSIONS

Let me conclude with two interlaced observations:

(i) We hear all the time about the asymmetry allegedly inherent in present-day LOAC, with the legal cards stacked in favor of the major powers at the expense of poor (militarily under-equipped) countries. Well, cyber warfare lends impoverished countries—ones possessing no aircraft carriers, no F-15s or 16s, and no cruise missiles—the opportunity of leveling the score. All that such a country needs is a few "whiz kids" who are capable of breaking the firewalls of the high and mighty, perhaps turning the tables on the latter. Inordinate computer dependency by the strongest nations of the world thus leads to a special vulnerability.[35]

(ii) The real challenge for Cyber Command, as I see it, is to make sure that nobody will be able to turn the tables on the United States, and that the United States—the most advanced in the world, not only in aircraft carriers, F-15s and 16s and cruise missiles, but also in cyberspace—can preserve its military superiority against all actual and potential adversaries. I sincerely hope that Cyber Command is not mesmerized by entitlements to intellectual property, but instead is preparing itself—through "war gaming"—for contingencies of real war. For, if you delete "war" from the equation of "war gaming," the only element that you are left with is "gaming." I believe that Cyber Command should shift its gaze away from the distractions of cyber operations in peacetime. It must focus on averting a future cyber Pearl Harbor.

---

34. *Procès-Verbal* Relating to the Rules of Submarine Warfare set forth in Part IV of the Treaty of London of 22 April 1930, Nov. 6, 1936, 173 L.N.T.S. 353, 3 Bevans 298, *reprinted in* THE LAWS OF ARMED CONFLICTS, *supra* note 21, at 1145, 1146.

35. *See* Robert G. Hanseman, *The Realities and Legalities of Information Warfare*, 42 AIR FORCE LAW REVIEW 173, 191–95 (1997).

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Cyber Warriors and the *Jus in Bello*

Vijay M. Padmanabhan

89 INT'L L. STUD. 288 (2013)

Volume 89 2013

Cyber Warriors and the *Jus in Bello*

Vijay M. Padmanabhan[*]

I. INTRODUCTION

The increasing interest in cyber operations, or "efforts to alter, disrupt, degrade or destroy computer systems or networks or the information or programs on them,"[1] as a warfighting tool raises questions regarding application of the *jus in bello* to "cyber warriors," or actors involved with cyber operations. Most cyber warriors will not be evaluated under the law of armed conflict. Cyber operations to date generally have amounted to nothing more than annoyances or crimes, or were in reality espionage, and therefore are regulated by municipal criminal law.[2] Where there is an armed conflict, most cyber operations and responses to cyber operations target

* Assistant Professor, Vanderbilt University Law School. Thanks to Ashley Deeks, Andy Grotto and Mike Newton for their helpful comments on this project.

1. *See* Matthew C. Waxman, *Cyber Attacks as "Force" under U.N. Charter Article 2(4)*, *in* INTERNATIONAL LAW AND CHANGING CHARACTER OF WAR 43 (Raul A. "Pete" Pedrozo and Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies) (defining "cyber-operations").

2. *See* James A. Lewis, *Cyber Attacks, Real or Imagined, and Cyber War*, CSIS (July 11, 2011), http://csis.org/publication/cyber-attacks-real-or-imagined-and-cyber-war (arguing against "hyperbole" in characterizing cyber operations as acts of war).

infrastructure and property, thereby bypassing the rules governing targeting of persons.

Nevertheless, the question of the legal status of cyber warriors under the *jus in bello* is likely to arise in two circumstances. First, the international armed conflicts and non-international armed conflicts of the present and the future are likely to include cyber operations as one element of an integrated war strategy. The 2008 armed conflict between Russia and Georgia over South Ossetia included large-scale distributed denial of service (DDS) attacks against Georgian government websites in an effort disrupt communication between the government and its people.[3] The relatively low cost of cyber operations compared to kinetic attacks suggests they are likely to be used, perhaps in more destructive ways, in future wars.[4]

Second, an isolated cyber operation may have sufficient kinetic effects to rise to the level of an "armed attack," justifying the use of force in lawful self-defense. The United States and Israel launched a cyber operation against Iran's burgeoning nuclear program that used malicious code to impede the functioning of Iran's centrifuges in order to secure additional time for negotiations over the future of Iran's nuclear capability.[5] This operation, code-named Olympic Games, led at least one scholar to argue that the United States and Israel committed an armed attack against Iran.[6] It is reasonable to assume that States may wish to use force in the future against those involved in such attacks, and indeed the United States has expressly reserved the right to do so.[7] Such force may amount to an "armed conflict" under the *jus in bello*, thereby raising issues as to the status of those targeted.

Under these two circumstances, categorization of cyber warriors as combatants, civilians or potentially unlawful combatants carries consequences. The most important of these are with respect to targeting. Com-

---

3. *See* John Markoff, *Before the Gunfire, Cyberattacks*, NEW YORK TIMES, Aug. 13, 2008, at A1 (describing attacks).

4. *See id.* (quoting expert comparing the low cost of cyber operations to the greater cost of kinetic operations).

5. *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES, June 1, 2012, at A1 (describing details of the Olympic Games program).

6. *See, e.g.,* Paul Rosenzweig, *The Stuxnet Story and Some Interesting Questions,* LAWFARE BLOG (June 2, 2012, 16:52 EDT), http://www.lawfareblog.com/2012/06/the-stuxnet-story-and-some-interesting-questions/ (arguing Olympic Games amounted to an "armed attack" against Iran as understood under the U.N. Charter).

7. *See* THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE 14 (2011) (reserving the right to use "all necessary means," including military force, to defend the United States and its allies from cyber operations).

batants, lawful or unlawful, are subject to targeting at all times during an armed conflict by virtue of their status. Civilians, by contrast, may not be made the object of attack,[8] except for such time as they directly participate in hostilities.[9] Civilians present during an attack also must be accounted for in the attacker's proportionality analysis, unless they are directly participating.[10] Consequences also arise with respect to the detention, treatment and prosecution of cyber warriors,[11] although their capture by the enemy is relatively unlikely.[12]

This article analyzes the difficult legal questions raised by application of the *jus in bello* categories to cyber warriors. The traditional category approach to targeting and detention works best when participation is limited to traditional combatants and it is possible to distinguish on the battlefield between combatants and civilians. Both assumptions are challenged in cyber operations.

First, actors other than traditional combatants are likely to play a significant role in cyber operations. The complex nature of cyber weapons may

8. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 51(2), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

9. *Id.*, art. 51(3).

10. *See id.,* art. 57(2)(b) (introducing the requirement of "proportionality").

11. Captured combatants may be detained until the end of hostilities. Lawful combatants enjoy immunity from prosecution in the national courts of the enemy State for actions undertaken consistent with the laws of war, and are entitled to prisoner of war privileges after capture. Knut Dörmann, *The Legal Situation of "Unlawful/Unprivileged Combatants,"* 85 INTERNATIONAL REVIEW OF THE RED CROSS 45, 45–46 (2003). Unlawful combatants, if the category exists, differ from lawful combatants in that they lack combatant immunity and are not entitled to prisoner of war privileges. Civilians, as "protected persons," by contrast may only be detained on the basis of an individualized determination that the security of the detaining power makes detention absolutely necessary, and it must cease when the need ends. Convention Relative to the Treatment of Civilian Persons in Time of War art. 42–43, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 31 [hereinafter GCIV]. Civilians are not entitled to prisoner of war privileges, and may be subject to prosecution in a capturing State's civilian courts based upon activities for which a combatant would be immune.

12. Physical capture of a cyber warrior will take place only if: (1) the individual is present within the attacked State or territory occupied by that State; (2) is captured as part of a military operation in another State; or (3) is brought within the jurisdiction of the attacked State through legal means, such as extradition, or unlawful means such as rendition. Capture is most likely where the cyber warrior acts independently or on behalf of a non-State actor such that the State where he is located will participate, cooperate or acquiesce with capture. Capture is exceedingly unlikely where the cyber warrior acts on behalf of a State engaged in an armed conflict and directs his attacks from that State.

result in States using contractors with technical expertise to modify continually the features of the weapon in order to overcome the defenses of the target, blurring the line between the traditional civilian task of weapons development and the traditional combatant task of weapons use.[13] In other instances, States may see an advantage in using non-State actors to launch cyber operations on their behalf in order to retain plausible deniability with respect to its role in the attack.[14] Civilians may also play an active role in defending critical networks against cyber operations, given that many attacks will be against dual-use infrastructure managed by civilians.[15]

Actors with no links to any State may become cyber warriors, either through participating in a cyber operation on behalf of an organized armed group involved in non-international armed conflict, or on their own due to sympathies for a belligerent. The reduced financial resources required for cyber operations compared to traditional kinetic operations of similar strength makes it more feasible for non-State actors to employ such operations.[16]

Second, it is harder to determine what particular role an individual plays in cyber operations as compared to traditional military operations. Cyber operations are potentially difficult to trace given the risk that they will utilize the infrastructure of unsuspecting third parties to mask their involvement.[17] Even if the attacks are traced to a particular State or organization,

---

13. *See* Sean Watts, *Combatant Status and Computer Network Attack*, 50 VIRGINIA JOURNAL OF INTERNATIONAL LAW 392, 409–10 (2010) (describing the need for continuous technical expertise in deployment of cyber weapons). The problems posed by contractors assuming traditional combat roles are not unique to cyber and have been discussed elsewhere in the literature.

14. *See* Gregory J. Rattray & Jason Healey, *Non-State Actors and Cyber-Conflict*, *in* AMERICA'S CYBER FUTURE: SECURITY AND PROSPERITY IN THE INFORMATION AGE 67, 73 (Kristin M. Lord & Travis Sharp eds., 2011) (speculating that Iran might use Hezbollah to launch cyber operations to avoid attribution to Iran).

15. Congress has recently been involved in an extensive debate regarding the role of private actors in defending U.S. information infrastructure from cyber operations. *See* Michael S. Schmidt, *Cybersecurity Bill is Blocked in Senate by G.O.P. Filibuster*, NEW YORK TIMES, Aug. 2, 2012, at A3 (describing disagreement over cybersecurity standards for cooperation between corporations and the government).

16. *See* Rattray & Healey, *supra* note 14, at 67 (arguing that there is tremendous potential for non-State actors to use cyber attacks).

17. This problem has attracted attention in the context of the *jus ad bellum*, where attribution is required in order to invoke the right of self-defense. *See* Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421, 443–44 (2011) (describing the effect of technical attribution problems on development of refinements to *jus ad bellum*).

resolving "doubt" as to whether the individual involved in the operation is targetable will be difficult to do.[18]

As a result, existing law provides at best imperfect guidance on targeting and, where relevant, detention decisions. While at least one scholar has suggested that these limitations with existing law demonstrate the need for an international "cyberspace treaty,"[19] the limited understand of the potential of cyber operations, the differing agendas of international actors on cyber questions and the contested nature of the legal issues all render completion of such a treaty highly unlikely. Instead, informal partnerships between like-minded States to develop joint strategies to handle cyber warriors may begin the process of developing new, more detailed rules regulating cyberspace.

II. LAWFUL COMBATANTS

Some subset of cyber warriors will qualify as lawful combatants subject to targeting at all times during an armed conflict and detention until the end of hostilities, but with the protection of combatant immunity and prisoner of war privileges if captured. These cyber warriors are formally integrated into the armed forces of a State under the domestic law of that State.[20] Their formal membership within the armed forces renders them non-civilians irrespective of their particular function with respect to the cyber operation.[21] Thus, the small cyber unit within United States Strategic Command involved in the Olympic Games attack would be composed of lawful combatants in an armed conflict with Iran, regardless of the particular function of any member of the unit with respect to the operation.[22]

---

18. *See* Additional Protocol I, *supra* note 8, art. 50(1) ("In case of doubt whether a person is a civilian, that person shall be considered to be a civilian."); art 52(3) (In case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used.").

19. Rex Hughes, *A Treaty for Cyberspace*, 86 INTERNATIONAL AFFAIRS 523, 524 (2010).

20. Additional Protocol I, *supra* note 8, arts. 43(1) & 44(1); Convention Relative to the Treatment of Prisoners of War art. 4(a)(1), Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GCIII].

21. *See* NILS MELZER, INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES 25 (2009) ("Members of regularly constituted forces are not civilians, regardless of their individual conduct or the function they assume within the armed forces.").

22. Article 46 of Additional Protocol I excludes members of the armed forces engaging in espionage from prisoner of war status. Such exclusion is potentially important to

But, as explained at the outset, States may employ in cyber operations at least three categories of actors who are not formally affiliated with the armed forces of the State. States may hire civilian contractors to design weapons that will be employed in a cyber operation.[23] While weapons design has traditionally been viewed as a civilian activity, cyber weapons are different from tanks or planes in that the weapon must itself be modified continuously to react to unexpected and evolving defenses within a specific target.[24] Such modifications require weapons designers to work much more directly with military and intelligence counterparts during the course of the attack, increasing the quality and intensity of their participation in the conflict.[25]

Second, States may use non-State actors to launch cyber operations in order to maintain plausible deniability for state responsibility purposes. For example, the Georgian government accused the Russian Federation of hiring criminal organizations and encouraging patriotic "hacktivists" to launch attacks against Georgia during the 2008 conflict over South Ossetia.[26]

Third, States may rely upon members of its civilian population to defend civilian infrastructure from incoming cyber operations. States increasingly rely upon private assets, such as fiber optics networks, Internet service providers and commercial data storage facilities, as dual-use infrastructure.[27] These assets can be targeted in cyber operations, placing the civilian ownership of these networks at the front lines of any defense effort. Such defense may be purely reactive, as the network operators merely try to mit-

---

cyber warriors because many cyber operations are accompanied by espionage. If captured by the enemy in an armed conflict, members of the armed forces engaged in espionage might not receive prisoner of war privileges and may be prosecuted. However, the military advantage of cyber espionage is that it can be conducted remotely, outside the territory of the spied upon State. Under such circumstances, the capture of a spying cyber warrior is unlikely. The loss of prisoner of war privileges is irrelevant to the right of the aggrieved State to target a spying member of the armed forces as part of an armed conflict.

23. Such contractors risk mercenary status if they are not nationals of the State, are motivated to participate in the conflict by desire for pecuniary gain and are paid compensation substantially in excess of that received by members of their armed forces of a similar rank. *See* Additional Protocol I, *supra* note 8, art. 47 (detailing requirements for mercenary status).

24. Watts, *supra* note 13, at 409–10.

25. *Id.* at 410.

26. *See id.* at 411 (quoting the chief of the Georgian National Security Council).

27. *See* Rattray & Healey, *supra* note 14, at 67 (explaining why non-State actors are likely to play an outsized role in cyber defense).

igate the effects of the attack.[28] But in other instances, those under attack may choose to counterstrike in an effort to end the attacks. Such an offensive response to attacks might be the cyber equivalent of traditional partisans taking up arms to protect their country in response to a kinetic attack.[29]

Such actors could be recognized as lawful combatants under the Third Geneva Convention.[30] Article 4(A)(2) provides that members of other militias "belonging to a Party to the conflict" are lawful combatants entitled to prisoner of war privileges provided that they are under responsible command, observe the principle of distinction by wearing a fixed sign and carrying arms openly, and conduct their operations consistent with the laws and customs of war. Cyber warriors involved in the design and launch of cyber weapons, as well as quasi-independent groups used to launch cyber operations, could conceivably meet these requirements.

Article 4(A)(6) grants inhabitants of a non-occupied territory prisoner of war status if they spontaneously take up arms to defend against invading forces, if they carry arms openly and respect the laws and customs of war. Civilians administering critical infrastructure who use active defenses to respond to a cyber operation might be categorized as a cyber *levée en masse*, and thereby entitled to combatant status.

Nevertheless, two difficulties exist with applying these provisions to cyber warriors. First, to qualify for lawful combatant status under Article 4(A)(2) the group in question must "belong to a Party to the conflict." The ICRC's *Interpretive Guidance* on direct participation in hostilities concludes that this standard is satisfied by a de facto relationship between the State and the group such that it is evident that the group conducts hostilities "on behalf and with the agreement of the Party."[31]

The International Criminal Tribunal for the former Yugoslavia Appeals Chamber in the *Tadić* case held that a State must exercise "effective control" over such a group for it to "belong to" the State. Effective control requires a relationship of "dependence and allegiance" with the State.[32] If

28. Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 1011, 1032–33 (2010).

29. *See id.* at 1033–35 (explaining why such an outcome may be more likely in the cyber realm).

30. GCIII, *supra* note 20.

31. MELZER, *supra* note 21, at 23.

32. Prosecutor v. Tadić, Case No. IT-94-1-l, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 94 (Int'l Crim. Trib. for the former Yugoslavia Oct. 2, 1995).

the State is using such a group to launch cyber operations to avoid State responsibility, then it may be very difficult to locate evidence to establish that the group is, in fact, acting under the "effective control" of the State.

Second, both 4(A)(2) and 4(A)(6) demand that lawful combatants abide by the principle of distinction, whether by wearing a fixed sign and/or carrying arms openly.[33] Literal application of these requirements to cyber warriors is likely to result in the conclusion that some of these actors are not lawful combatants. They are unlikely to wear uniforms, given that they are not part of the armed forces of the State. They are also likely to hide the military nature of computers used in a cyber operation by employing the outward markings of civilian computer infrastructure, such as a civilian Internet Protocol (IP) address.

Scholars have argued that these distinction requirements are antiquated with respect to cyber operations because cyber operations are launched remotely; the failure of a cyber warrior to wear a uniform, for example, does not provide him an inappropriate military advantage by appearing to blend with the civilian population.[34] Heather Dinniss writes that a potential update to these provisions in the context of cyber would be to mandate that cyber operations be launched from a computer with a military IP address in order for the cyber warrior to receive combatant status.[35] She questions, however, the practicality of such a requirement, explaining that a military IP address would place an immediate target on the computer involved in an attack.[36]

Query, however, whether this result is any different from the target a soldier in a traditional conflict places on himself by wearing a uniform and carrying his arms openly. A requirement that in order to be a lawful com-

---

33. There is a vigorous legal debate about whether these requirements must be met by regular armed forces as well in order to qualify as lawful combatants. *Compare* Sean D. Murphy, *Evolving Geneva Convention Paradigms in the War on Terrorism: Applying the Core Rules to the Release of Persons Deemed "Unprivileged Combatants,"* 75 GEORGE WASHINGTON LAW REVIEW 1105, 1127–28 (2007) (arguing yes), *with* Evan J. Wallach, *Afghanistan, Quirin and Uchiyama: Does the Sauce Suit the Gander?*, 2003 ARMY LAWYER, Nov. 2003, at 18, 24 (arguing no).

34. *See* HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 145 (2012) (describing usefulness of literal application of requirements of having a fixed distinctive sign recognizable at a distance and carrying arms openly as "diminished" with remote attacks); Watts, *supra* note 13, at 440 (same).

35. DINNISS, *supra* note 34, at 146.

36. *Id.* ("requiring a computer to be marked as a military computer is tantamount to painting a bulls-eye").

batant a cyber warrior must use a military IP address in his attacks incentivizes transparency in cyber operations. Transparency mitigates the risk that an attacked State would retaliate against a third State or civilian infrastructure not actually involved in a cyber operation because of a false IP address.

III. CIVILIANS

The analysis in Part II suggests that some subset of cyber warriors with an affiliation or sympathy toward a State in an armed conflict may not be lawful combatants. There are other similarly situated cyber warriors.

Cyber warriors engaged in cyber operations on behalf of non-State groups which are engaged in non-international armed conflict are not to be entitled to lawful combatant status because they do not "belong to" a State party to the conflict. For example, members of al Qaida have admitted to engaging in "low-level and disruptive" cyber operations including sabotage of political websites and denial of service attacks as part of their organization's war with the United States.[37] Such individuals, even if part of the armed wing of al Qaida, would not qualify for lawful combatant status.

"Hacktivists," or non-State actors unaffiliated with either side in an armed conflict who undertake cyber operations out of personal sympathies with a belligerent also do not qualify for combatant status because they lack a relationship with a State party to the conflict. One explanation for the DDS attacks directed against Georgian websites is that they were launched by the nationalist Russian hacker community, which may have been tipped off by the Russian government about plans to use force in South Ossetia.[38] Such a loose affiliation with the State is unlikely to meet the standard for "belonging to a Party" to the conflict because hacktivists are not under the "effective control" of the State.

Some scholars[39] and the Israeli Supreme Court[40] have taken the position that anyone who is not a lawful combatant is a civilian. The Interna-

37. *See* Rattray & Healey, *supra* note 14, at 72 (quoting statements of Guantanamo detainee Mohamedou Ould Slahi describing al Qaida's cyber capabilities).

38. *See* PAUL CORNISH ET AL., CHATHAM HOUSE, ON CYBER WARFARE 6 (2010) (detailing attacks by private Russian groups on Georgia and Estonia).

39. *See, e.g.,* Marco Sassòli, *Use and Abuse of the Laws of War in the "War on Terrorism,"* 22 LAW & INEQUALITY 195, 207–08 (2004) (listing scholarly support for this position).

40. *See* HCJ 769/02 Public Committee against Torture in Israel v. Government of Israel 2006(2) PD 459, ¶ 28 [2006] (Isr.), *reprinted in* 46 INTERNATIONAL LEGAL MATERIALS

tional Committee for the Red Cross (ICRC) *Commentary* on Geneva Convention IV (GCIV) indicates that it was the intention of the drafters of the Geneva Conventions to cover everyone within the ambit of the treaties, either as a prisoner of war or as a civilian.[41] Such a view draws support from the text of GCIV, which does not expressly exclude those engaged in fighting from protected person status and does contemplate "spies and saboteurs" achieving that status in occupied territory.[42]

If cyber warriors are civilians, they would be subject to targeting only "for such time as" they "directly participate in hostilities."[43] The content of the direct participation standard is the subject of significant legal debate. The ICRC issued *Interpretive Guidance* on the content of the terms,[44] which in turn has spawned numerous scholarly critiques of both the process by which the *Guidance* was created and its content.[45] Nevertheless, it is useful to consider some of the challenges in applying the components of direct participation identified by the ICRC to cyber warriors in an effort to understand what may be at stake in categorizing them as civilians.[46]

The *Interpretive Guidance* provides that a civilian directly participates in hostilities when he (1) engages in an act that directly causes (2) harm of a

373 (2007) (treating Palestinian militants as civilians because it did not see a basis for recognizing a category other than lawful combatant and civilian).

41. *See* COMMENTARY: IV GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PROTECTED PERSONS IN TIME OF WAR 51 (Jean S. Pictet ed., 1960) [hereinafter FOURTH GENEVA CONVENTION COMMENTARY] ("Every person in the hands of the enemy must have some status under international law."). In addition to prisoner of war and civilian, Pictet explained that an individual could also be protected under the First Geneva Convention as medical personnel. *Id.*

42. GCIV, *supra* note 11, art. 5. *See also* FOURTH GENEVA CONVENTION COMMENTARY, *id.* at 53 (defending the need to provide spies and saboteurs "protected person" protections).

43. Additional Protocol I, *supra* note 8, art. 51(3).

44. MELZER, *supra* note 21.

45. *See generally* Ryan Goodman & Derek Jinks, *The ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law: An Introduction to the Forum*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 637 (2010) (summarizing a range of perspectives on the *Interpretive Guidance*).

46. Categorizing cyber warriors as civilians also has consequences for detention. Civilian protected persons may be detained only for imperative reasons of security, unlike combatants who may be detained for the duration of hostilities without individualized reason. *See* GCIV, *supra* note 11, art. 42 (permitting detention of civilians when demanded by security). But as discussed above, cyber warriors are unlikely to be detained under the laws of war given the difficulties inherent in their capture, and therefore this article focuses on consequences for targeting.

sufficient gravity with (3) the intent of aiding a belligerent party. Application of each of these terms to cyber warriors raises difficult legal questions.

The ICRC argues "direct causation" is satisfied where the participation in question causes the requisite level of harm in "one causal step."[47] Such a requirement distinguishes between acts like scientific research and weapons design, which require further action to bring the harm to fruition and are not direct participation, and the deployment of weapons themselves, which causes the harm in question, and is direct participation.[48]

The "direct causation" requirement appears easier to meet in the context of cyber operations than in traditional kinetic operations. Cyber weapons by their nature require constant modifications to overcome the active defenses of the target. As a result, those designing weapons may be called upon to operationalize their weapon, using intelligence about the target to do so.[49] The increased depth and quality of such participation may meet the "direct causation" standard because the act of modifying cyber weapons during the course of an operation to overcome system defenses is "one causal step" away from the harm in question. Indeed, the *Interpretive Guidance* explains that production of weapons "carried out as an integral part of a specific military operation" meets the causation requirement.[50]

Such an outcome raises concerns from the perspective of those favoring a more robust role for human rights protections in warfighting. One concern raised about the ICRC *Guidance* is that it defines direct participation too broadly, in the process opening up too many civilians to the use of force.[51] To the extent cyber warriors blur the line between combatant and civilian and are therefore subject to targeting, these worries are exacerbated.

The "threshold of harm" limits direct participation to acts that either are likely to affect the military operations or military capacity of a party to an armed conflict, or which result in death or injury to civilians or destruction of civilian property. The ICRC *Guidance* specifically states that attacks on the computer networks of the military can be sufficiently grave to con-

---

47. MELZER, *supra* note 21, at 53.

48. *See id.* (distinguishing general design and transport of weapons from their use in specific military operations).

49. *See* Watts, *supra* note 13, at 410 (claiming civilians "are likely to participate in a more direct and ongoing fashion" with cyber weapons).

50. MELZER, *supra* note 21, at 53.

51. *See* Goodman & Jinks, *supra* note 45, at 639 (describing concerns of human rights actors with the ICRC *Guidance*).

stitute direct participation.[52] But the *Guidance* rejects the idea that "manipulation" of civilian computer networks passes the threshold of harm requirement, unless the result is destruction of civilian infrastructure.[53]

The threshold of harm standard has the potential to distinguish between the participation of different categories of cyber warriors. Cyber warriors involved in exploitation of military and government systems to obtain tactical intelligence information or destroy military infrastructure will see their acts pass the requisite threshold of harm, and thus be subject to targeting provided the remaining criteria are met. By contrast, those exploiting civilian systems for the purpose of harming the economic prospects of an enemy State would likely not meet the threshold of harm, unless they destroy civilian infrastructure in the process of doing so.

Michael Schmitt has criticized the threshold of harm standard for being "under-inclusive" in terms of the conduct included within the ambit of direct participation. Schmitt questions why the *Interpretive Guidance* limits participation to acts that cause "death, injury, or destruction" to civilians and civilian property, as opposed to including any harmful acts directed against protected persons and objects that are part of war strategy or are evidently related to ongoing hostilities.[54] Application of the threshold of harm standard to cyber warriors demonstrates the strength of these concerns. Cyber warriors are free to engage in cyber operations that could exact a significant toll on the civilian population of the enemy State without risk of being targeted, a consequence seemingly at odds with the goal of protecting civilians from the consequences of armed conflict.

The requirement of "belligerent nexus" requires that an act of direct participation be objectively intended to cause the requisite threshold of harm in aid of a party to a conflict. Such a requirement is designed in part to weed out unrelated but coterminous violence, such as a bank robbery in a war zone. In the context of cyber warriors the requirement would distinguish between patriotic hacktivists objectively seeking to aid their country

52. *Id.* at 48.

53. *See id.* at 50 (comparing manipulation of civilian computer networks to building fences or roadblocks, disrupting food or electrical supplies, appropriating property or arresting and deporting civilians).

54. Michael N. Schmitt, *Deconstructing Direct Participation in Hostilities*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 697, 724 (2010).

in war and groups like Anonymous[55] that may commit very similar attacks but with no intention to benefit belligerents.

This requirement may produce some unusual, and arguably inequitable, results when applied to cyber. Anonymous threatened to launch a cyber operation against the Pentagon over its continued detention of Private First Class Bradley Manning because of his involvement in the WikiLeaks affair.[56] If such an operation were launched by an al Qaida cyber unit as part of its armed conflict with the United States, then al Qaida warriors involved in the operation would meet the belligerent nexus requirement. By contrast, members of Anonymous, motivated by free speech concerns, would not, even if their attack would have similarly problematic consequences for the U.S. effort to combat al Qaida. Such disparate outcomes may be justifiable in the context of kinetic attacks, where States may have law enforcement options with respect to mitigating the threat posed by actors lacking requisite belligerent nexus. But such an outcome is harder to stomach in the cyber context, given that such attacks may emanate from outside the State, leaving States with few alternatives to force to mitigate the threat.

The direct participation standard also imposes temporal limitations on targeting civilians. Additional Protocol I permits targeting of directly participating civilians only "for such time" as they directly participate. What might this standard mean in the context of cyber? Consider that a State may not be aware of a cyber attack until long after the participation of any of the actors involved in the attack has terminated. Iran, for example, was not aware that the problems with its centrifuges were related to foreign sabotage until well into the Olympic Games program.[57] Strict interpretation of the "such time" language could well insulate civilians involved in programs like Olympic Games from targeting by States. The ICRC *Guidance* appears to endorse this result, stating "with computer network attacks . . . the duration of direct participation in hostilities will be restricted to the

---

55. Anonymous describes itself as "a decentralized network of individuals focused on promoting access to information, free speech, and transparency." *About Us*, ANONYMOUS ANALYTICS, http://anonanalytics.com/ (last visited Nov. 9, 2012). *See also* Scott Neuman, *Anonymous Comes Out in the Open*, NPR (Sept. 16, 2011, 5:02 PM), http://www.npr.org/2011/09/16/140539560/anonymous-comes-out-in-the-open (describing Anonymous as a "cyberguerilla" group).

56. *See* Michael Stone, *Pentagon Fears Anonymous Attack, re: WikiLeaks, Bradley Manning*, EXAMINER (Mar. 9, 2011), http://www.examiner.com/article/pentagon-fears-anonymous-attack-re-wikileaks-bradley-manning.

57. *See* Sanger, *supra* note 5 (describing initial reaction of Iranian officials to Stuxnet).

immediate execution of the act and preparatory measures forming an integral part of that act."[58]

Heather Dinniss suggests that the temporal duration of a cyber operation could include the time during which the effects of the cyber weapon are being felt. Dinniss explains such an interpretation is consistent with the nature of a cyber operation: the operation is ongoing as long as the cyber weapon is acting against the computer system of the enemy, much as a kidnapping goes on during the entire length a person is held hostage. This interpretation of the temporal limitations of the direct participation standard would better protect the ability of belligerents to target those involved in cyber operations that have a continuing adverse effect on military operations. It would also potentially discourage civilian participation, a core goal of international humanitarian law (IHL).

IV. UNLAWFUL COMBATANTS

There are, however, significant inequities that result from treating cyber warriors as civilians. Limiting targeting to such time as cyber warriors directly participate, and including them in a proportionality analysis gives such individuals greater protections from targeting than lawful combatants. Such a rule creates an incentive for cyber units to avoid following the distinction and attribution rules needed for lawful combatant status.[59] This perverse incentive is stronger in the cyber context than elsewhere because cyber warriors are unlikely to be captured, and therefore to need the combatant immunity and prisoner of war privileges that come with being labeled a lawful combatant. The inequities that result from treating irregular fighters as civilians explain the position of at least some States during the negotiations of the Fourth Geneva Convention against doing so.[60]

Instead, some scholars and States argue that international law recognizes a third category for targeting and detention purposes: "unlawful combat-

58. MELZER, *supra* note 21, at 68.

59. *See* Richard D. Rosen, *Targeting Enemy Forces in the War on Terror: Preserving Civilian Immunity*, 42 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 683, 736–39 (2009) (describing difficult consequences that result from treating non-State soldiers as civilians).

60. *See* 2 FINAL RECORD OF THE DIPLOMATIC CONFERENCE OF GENEVA OF 1949, sec. A, at 621 (1949) (quoting British delegate explaining "the whole conception of the Civilian Convention was the protection of civilian victims of war and not the protection of illegitimate bearers of arms").

ant" or "unprivileged belligerent."[61] Unlawful combatants are subject to targeting at all times as are lawful combatants.[62] They are also not included as collateral damage in the targeting proportionality determination. This categorization would eliminate an incentive for cyber warriors to avoid meeting the requirements for lawful combatant status.

Given the varied groups of cyber warriors described in Parts I and II who are not entitled to lawful combatant status, the category of unlawful combatant must distinguish between those who should be subject to targeting at all times during the armed conflict, and those who deserve the protections afforded civilians. Unfortunately, there is no agreed test within international law as to when an individual becomes an unlawful combatant. The debate over categorization of irregular fighters in the post-9/11 conflicts has led to debate over the potential boundaries for such a category.

The ICRC's *Interpretive Guidance* categorizes those whose "continuous function involves the preparation, execution, or command of acts or operations amounting to direct participation" as combatants.[63] It would distinguish these individuals from "recruiters, trainers, financiers and propagandists," who contribute to the war effort, but in a manner more akin to civilian supporters than combatants.[64]

Of most interest in the context of cyber operations is that the *Guidance* considers the purchase, manufacturing and maintenance of weapons outside of a specific military operation, as well as the collection of intelligence that is not tactical in nature, to be civilian functions. Under this approach categorizing cyber warriors would turn largely on whether they have regu-

---

61. This was the approach taken by the Bush administration to categorize members of the Taliban and al Qaida in the post-9/11 conflicts. Memorandum from President George W. Bush to the Vice President et al. on Human Treatment of al Qaeda and Taliban Detainees ¶ 2(d) (Feb. 7, 2002), *available at* http://www.washingtonpost.com/wp-srv/nation/documents/020702bush.pdf. While controversial, this category has a long historic pedigree. *See* John B. Bellinger III & Vijay M. Padmanabhan, *Detention Operations in Contemporary Conflicts: Four Challenges for the Geneva Conventions and other Existing Law*, 105 AMERICAN JOURNAL OF INTERNATIONAL 201, 217 n.80 (2011) (describing extensive support for the existence of this category).

62. Unlawful combatants are subject to detention based on their status as combatants until the end of hostilities. But they do not enjoy combatant immunity, meaning they are subject to prosecution in the civilian courts of the enemy State for actions taken during combat. They are also not entitled to prisoner of war privileges.

63. MELZER, *supra* note 21, at 27.

64. *Id.* at 34.

lar, operation-specific roles in the unit or general support roles.[65] Thus, a computer specialist whose role is limited to designing cyber weapons or collecting information about the nature of enemy infrastructure would be a civilian. By contrast, a similar specialist who modifies viruses to overcome the active defenses of the target, or who collects information about those defenses in order to operationalize an attack, would be considered a combatant.

Scholars have criticized this approach for being unduly restrictive in assigning combatant status to those in armed groups. Kenneth Watkin argues that it is artificial to divide integrated units that work together to accomplish a military objective into a mix of combatants and civilians. For example, he notes that crews that plant improvised explosive devices in Iraq and Afghanistan are units unto themselves, with different individuals within the unit responsible for weapons production, training, intelligence gathering and actual weapons launch. Watkin argues that to limit combatant status to triggermen is artificial, as the unit as a whole must be targetable in order to mitigate its threat.[66]

Watkin's criticism is somewhat less trenchant in the context of cyber weapons. The potentially complex nature of cyber weapons may require a blending of duties between those involved in attack preparation and launch, such that most members of a cyber unit would be sufficiently involved with a specific operation to be deemed combatants. Nevertheless, it is legitimate to question whether dividing members of a cyber unit based on function accurately reflects the cohesive, integrated threat such a unit poses to enemy infrastructure.

A different approach was tentatively explored by the D.C. District Court in the Guantanamo habeas cases. Two district court judges crafted a test that permitted the government to detain as enemy combatants those who receive and execute orders from the enemy's command structure because such individuals are within the "armed forces" of enemy non-State

65. Of course, hacktivists by definition have no "regular role" within any belligerent armed forces, and would thus be treated as civilians under this analysis. Similarly, those whose primary role is to guard civilian infrastructure but who get drawn into conflict while defending that infrastructure have no role in the belligerent armed forces and would be civilians, unless deemed part of a *levée en masse*.

66. *See* Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC Direct Participation in Hostilities Interpretive Guidance*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 641, 680–82 (2010) (criticizing "continuous combat function" test as applied to irregular units).

organizations.[67] By contrast, those who merely supported the enemy through functions like propaganda or finance were not detainable as combatants.[68]

Such an approach applied to cyber warriors would allow entire cyber units, such as quasi-independent groups or contractors affiliated with a belligerent in an armed conflict, to be considered combatants if, in fact, the unit took orders and responded to orders from the belligerent. However, efforts by belligerents to mask their relationship with a cyber unit could make application of this test difficult. Targeting decisions will not be made with the benefit of the extensive process used in the detention context, where administrative or even court review is possible.

The key point is if cyber warriors can be categorized as unlawful combatants, then parameters for that category must be identified.

V. PROCESS

The fluid and imprecise nature of the categories described in Parts II–IV raise a difficult question: how will an actor deciding whether to use force obtain sufficient information to determine how to categorize a cyber warrior? Article 57(2) of Additional Protocol I mandates that those making targeting decisions "do everything feasible" to verify that the subject of the attack is not a civilian who is not directly participating in hostilities. International law recognizes that factors such as "time constraints, risks, technology, and resource costs" condition the obligation to obtain information to aid the targeting decision.[69] Thus, doing what is "feasible" to distinguish civilians requires exercising "reasonable care" in targeting decisions.[70]

---

67. Gherebi v. Obama, 609 F. Supp.2d 43, 68–70 (D.D.C. 2009); Hamlily v. Obama, 616 F. Supp.2d 63, 67–69 (D.D.C. 2009).

68. A panel of the U.S. Court of Appeals for the D.C. Circuit ultimately rejected the use of a detention standard based upon the IHL definition of "combatant." Al-Bihani v. Obama, 590 F.3d 866, 871 (2010). While the D.C. Circuit sitting *en banc* suggested this part of the opinion was dictum. Al-Bihani v. Obama, 619 F.3d 1, 1 (D.C. Cir. 2010) (Sentelle, J., concurring in denial of rehearing *en banc*), the Appeals Court has relied on *Al-Bihani* to reject the use of the command structure requirement as a limitation on the executive's detention authority. Awad v. Obama, 608 F.3d 1, 11–12 (D.C. Cir. 2010); Bensayah v. Obama, 610 F.3d 718, 725 (D.C. Cir. 2010).

69. *See* Matthew C. Waxman, *Detention as Targeting: Standards of Certainty and Detention of Suspected Terrorists*, 108 COLUMBIA LAW REVIEW 1365, 1389 (2008) (describing limits on State obligations in targeting decisions).

70. *See id.* at 1388 (marshaling evidence to support this standard).

Exercising reasonable care in the cyber context requires evaluating factors such as:[71]

- Affiliation between the cyber warrior and the belligerent;
- The function the cyber warrior serves within a cyber unit;
- Whether the cyber warrior's act "directly caused" the harm in question; and
- Whether the cyber warrior's participation in the hostilities continues.

These determinations are difficult because cyber warriors expend great effort to mask their identity. They also act in civilian environments far from any real battlefield, which raises the risk of misidentification.[72]

U.S. officials have yet to provide any guidance on what procedures the United States would employ before targeting an individual or property believed to be involved in a cyber attack on the United States. U.S. State Department Legal Adviser Harold Koh contends that this problem is a "technical and policy" challenge for States seeking to follow international law in responding to cyber attacks.[73] Development of procedural standards governing the targeting of cyber warriors is essential to reducing the legal uncertainties surrounding cyber operations.

Perhaps the closest analogy for targeting purposes is the procedures employed by the United States in its drone program targeting members of al Qaida in Yemen and Pakistan. While the exact nature of the inquiry conducted by U.S. officials to determine whether potential targets are lawful remains secret, Obama administration officials have indicated it involves

---

71. The process question is easier in the context of detention. One of the lessons emerging from the post-9/11 conflicts is that adversarial administrative and court procedures can be employed to reduce the risk of erroneous deprivations of liberty where there is serious risk of misidentification of alleged combatants. *See* Bellinger & Padmanabhan, *supra* note 61, at 221 (criticizing the decision of the Bush administration to provide minimal process to detainees in the conflict with al Qaida and the Taliban). The technical nature of cyber operations suggests that there may be the need for technical witnesses in determining whether a captured cyber warrior is a combatant or a civilian.

72. *See* Vijay M. Padmanabhan, *Legacy of 9/11: Continuing the Humanization of Humanitarian Law*, 14 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 419, 421–22 (2011) (describing a similar problem in the context of conflicts with non-State actors).

73. *See* Harold H. Koh, Legal Adviser, U.S. Department of State, International Law in Cyberspace, Remarks at the USCYBERCOM Inter-agency Legal Conference (Sept. 18, 2012) (describing challenges the United States faces in applying international law to cyber-conflicts).

assessment of intelligence information by a range of government officials, including the President himself.[74]

Targeting suspected cyber warriors will require a potentially more robust process, given the greater ease with which cyber fingerprints can be hidden and the technical nature of the attribution inquiry. But given that cyber operations can be part of more intense, ongoing armed conflicts than the U.S. conflict with al Qaida, such added process may not be realistic. For example, in the cataclysmic event of an armed conflict between the United States and China it would be unrealistic to expect high ranking government officials to spend time evaluating the decision to target individual cyber warriors.

VI. THE FUTURE

This article reveals the large number of difficult legal questions that arise when attempting to categorize cyber warriors for *jus in bello* purposes during an armed conflict. Some of these questions are particular to cyber; other questions reflect general lacunae in the law of armed conflict that have resonance in cyber operations. These questions include:

- When does a cyber warrior "belong to" a belligerent to the conflict?
- Must a cyber warrior affiliated with a State party distinguish himself visually in order to be categorized as a lawful combatant?
- Are all cyber warriors who are not lawful combatants civilians?
- If there is a category of unlawful combatants, what parameters define that category and how do those parameters apply to cyber warriors?
- How should the concept of direct participation in hostilities, including its temporal dimension, be applied to cyber warriors?
- What process should be implemented to resolve distinction questions in targeting?

---

74. *See* John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism, The Ethics and Efficacy of the President's Counterterrorism Strategy, Remarks at the Woodrow Wilson International Center for Scholars (Apr. 30, 2012), *available at* http://www.wilsoncenter.org/event/the-efficacy-and-ethics-us-counterterrorism-strategy (providing bare bones account of targeting process); Jo Becker & Scott Shane, *Secret 'Kill' List Proves a Test of Obama's Principles and Will*, NEW YORK TIMES, May 29, 2012, at A1 (describing process in which Obama administration officials, including the President, debate the merits of killing potential targets in Yemen and Pakistan).

Given this multitude of questions, it is not surprising that scholars have begun to call for new international law to regulate cyberspace. Rex Hughes from the University of Cambridge has advocated for a multilateral treaty governing cyberspace.[75] Among the issues Hughes envisions such a treaty addressing is how to apply the principle of distinction to cyber warriors, including what, if any, modifications need to be made to rules distinguishing combatants from civilians.[76] In Hughes' favor is the current uncertain climate surrounding cyber capabilities. A world without clear understanding of relative cyber powers might be one that is willing to enter into an international agreement restricting and regulating its use. In this sense, we may in fact be, to steal a term from John Rawls, in a cyber "original position."

That said, there are at least two good reasons to be dubious about the prospects for a cyberspace treaty. First, as noted earlier, many of the questions that are contested in the area of cyber warriors are also contested in other areas of armed conflict. For example, conflicts with non-State actors like al Qaida have raised panoply of similar questions.[77] The fact that these questions are disputed in IHL writ large suggests that their resolution in a cyber treaty would be provocative and unlikely to attract international agreement.

Second, even at this early date there are significant disagreements about what regulation of cyberspace will look like. The British government has initiated an international forum to discuss regulation of cyberspace. That forum has already revealed deep disagreement about the areas of cyber most in need of regulation. Western States, including the United Kingdom and the United States, stress the need to protect computer networks and technological infrastructure from espionage and attack. China and Russia, by contrast, emphasize the need to regulate the dissemination of information across cyberspace, regulations that are anathema to the free speech human rights norm.[78] Failure to agree on the goals for regulation demonstrates how far apart the international community is on cyber regulation.

Instead there is a need for like-minded States actively grappling with cyber operations to think together about what form of future international

---

75. Hughes, *supra* note 19, at 524.

76. *See id.* at 537 (including distinction in issues for a future treaty).

77. *See generally* Bellinger & Padmanabhan, *supra* note 61 (describing areas of international law in need of further legal development to regulate conflicts with non-State actors).

78. *See* Nick Hopkins, *Britain in Talks on Cybersecurity Hotline with China and Russia*, GUARDIAN (Oct. 3, 2012), http://www.guardian.co.uk/politics/2012/oct/04/britain-cybersecurity-hotline-china-russia (describing areas of disagreement on cyber regulation).

regulation makes sense. Adam Segal and Matthew Waxman of the Council on Foreign Relations have argued that at this time the most that can be accomplished globally is for like-minded States to form partnerships on cybersecurity from which shared understandings on the use of force in response to cyber operations may emerge.[79] Including discussion of the legal problems created by cyber warriors will bolster the ability of IHL to remain relevant in regulating this rapidly changing area of warfighting.

79. *See* Adam Segal & Matthew Waxman, *Why a Cybersecurity Treaty is a Pipe Dream*, CNN WORLD (Oct. 27, 2011, 2:01 PM), http://globalpublicsquare.blogs.cnn.com/2011/10/27/why-a-cybersecurity-treaty-is-a-pipe-dream/.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests?

John F. Murphy

89 INT'L L. STUD. 309 (2013)

Volume 89 2013

Cyber War and International Law: Does the International Legal Process Constitute a Threat to U.S. Vital Interests?

John F. Murphy[*]

I. INTRODUCTION

As the concluding speaker at the conference on "Cyber War and International Law," co-sponsored by the Naval War College and the United States Cyber Command, Yoram Dinstein, Professor Emeritus at Tel Aviv University, professed some disappointment that there had not been a more extensive and sharper focus at the conference on "war."[1] But perhaps the limited amount of discussion of cyber "war" at the conference was a result of the reality that the international law issues arising from the possibility of war or armed conflict through cyber means have not been the primary concern of States and scholars faced with the challenges of the cyber threat. Rather, at least in the United Nations General Assembly and other international fora, such as the International Telecommunications Union (ITU), the threat posed by such adversaries of the United States as the Russian Federation and China seems to be an effort to adopt a global treaty

* Professor of Law, Villanova School of Law. I want to acknowledge the excellent research assistance of Lori Strickler, Reference Librarian, Villanova University School of Law; and Daria Hafner and Karrie Gurbacki, both second-year students at Villanova University School of Law.

1. See Yoram Dinstein, *Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference*, 89 INTERNATIONAL LAW STUDIES 276 (2013).

that would arguably allow increased regulation by the United Nations—and perhaps the ITU—that would endanger the free flow of information on the Internet and such basic values as privacy and freedom of speech. To be sure, a hostile takeover of the Internet could have serious implications for U.S. vulnerability to cyber attack and thereby amount to a serious threat to its national security, but this is a far cry from possible revisions of the *jus ad bellum* and *jus in bello* associated with cyber war, which is to the disadvantage of the United States.

The title of this article poses the question whether, in the context of cyber war and other related forms of cyber attack, the international legal process itself may pose a threat to vital U.S. interests. Certainly, as we shall see below, a successful effort by the Russian Federation and China to conclude a widely adopted global treaty authorizing the United Nations or the ITU to regulate the Internet would constitute such a threat. Moreover, in *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory,*[2] the International Court of Justice (ICJ) in an advisory opinion stated that "Article 51 of the Charter thus recognizes the existence of an inherent right of self-defence in the case of armed attack by one State against another State. However, Israel does not claim that the attacks against it are imputable to a foreign State."[3]

Similarly, in *Armed Activities on the Territory of the Congo,*[4] the ICJ rejected Uganda's claim that it had engaged in lawful military activity in Congo's territory to protect itself against insurgents who had organized themselves there to commit armed attacks against Uganda's territory. If the Court's viewpoint is correct, this would have very serious implications for the right of self-defense against cyber attacks because many, perhaps most, of such attacks are committed by non-State actors. The problem is compounded by the often present difficulty in determining who or what actually engaged in the attack (the problem of attribution). Fortunately, for reasons considered later in this article, the Court's viewpoint, which has been subject to withering criticism, is almost surely not correct. But the primary point to take away here is that one of the most important actors in the international legal process, the ICJ, has adopted a legal position that greatly threatens vital

2. Legal Consequences of the Construction of Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136 (July 9).

3. *Id.* ¶ 139.

4. Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168 (Dec. 19).

U.S. interests, as well as those of many other States in the international community.[5]

Speaking of vital U.S. interests, there have been recent developments in cyber space that raise the issue of U.S. interests in sharp relief. These developments involve four (apparently) State-sponsored computer viruses with the nicknames Stuxnet, Duqu, Flame and Gauss. The goals behind the development of these viruses vary. Stuxnet, for example, first became public knowledge in July 2010. It has been described as "far more complex than run-of-the mill hacker tools" and as

> a self-replicating worm that targeted programmable logic controllers (PLCs), the simple computers used to perform automated tasks in many industrial processes. PLCs are part of industrial control systems, most commonly referred to as Supervisory Control and Data Acquisition (SCADA) systems. SCADA systems are critical to the modern industrial world, controlling such things as water plants, auto manufacturing, and electrical power grids.[6]

According to the same commentator,

> [t]he Stuxnet code showed up on computer systems around the world, where it parked on hard drives, remaining inert if it did not find what it was seeking. The numbers indicate it was aimed at Iran; nearly 60 percent of reported Stuxnet infections occurred on systems in Iran. In fact, at least one system Stuxnet was programmed to target [were] controlled centrifuges critical to the production of nuclear material. It appears that Iran's uranium enrichment facility at Natanz was the specific target."[7]

In other words, the purpose behind Stuxnet was to undermine the Iranian nuclear program which, it is believed, is designed to produce a nuclear bomb. According to reports,[8] a series of Stuxnet attacks temporarily took

---

5. For analysis and criticism of other decisions and advisory opinions of the ICJ that arguably undermine the vital interests of States, see JOHN F. MURPHY, THE EVOLVING DIMENSIONS OF INTERNATIONAL LAW: HARD CHOICES FOR THE WORLD COMMUNITY 65–75 (2010).

6. Gary D. Brown, *Why Iran Didn't Admit Stuxnet Was an Attack*, JOINT FORCES QUARTERLY, Oct. 2011, at 70, *available at* http://www.ndu.edu/press/why-iran-didnt-admit-stuxnet.html.

7. *Id.*

8. *See* David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES, June 1, 2012, at A1, *available at* http://www.nytimes.com/2012/06/01/

out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium. As to who was behind these Stuxnet attacks, although the evidence is not entirely conclusive, there are numerous indications it was the United States and Israel.[9]

In contrast to Stuxnet, it appears the primary purpose behind the Doqu, Flame and Gauss viruses is cyber espionage. For example, a *Washington Post* article reported that the United States and Israel developed the Flame virus to gather intelligence "in preparation for cyber-sabotage aimed at slowing Iran's ability to develop a nuclear weapon."[10]

There is substantial support for the proposition that international law does not regulate espionage, although as is shown below, this proposition is controversial. There is also an issue whether, in any event, the same can be said of cyber espionage.

This article begins with a discussion of the legality (or not) of Stuxnet and the other recently developed viruses under current international law, specifically the *jus ad bellum* and the *jus in bello,* as well as an analysis of whether traditional forms of espionage or the emerging practice of cyber espionage are covered by current international law. It then turns to an examination of recent efforts by Russia, China and others to develop an international law treaty for regulating the Internet, and efforts by Russia in particular to conclude a treaty on cyber war, and the extent to which these efforts may represent a use of the international legal process that threatens U.S. vital interests. Next the article explores some of the legal implications of the claim that the United States has conflated the terms "use of force" in Article 2(4) and "armed attack" in Article 51 of the UN Charter in such a way as to support an overly expansive interpretation of the right of self-defense under Article 51. Lastly, the article considers some of the challenges that the use of cyber warfare by terrorists may pose to international law and policy.

---

world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r= 0.

9. *Id.*

10. *See* Ellen Nakashima, Greg Miller & Julie Tate, *U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say*, WASHINGTON POST (June 19, 2012), http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html.

II. THE COMPATIBILITY OF STUXNET WITH CURRENT INTERNATIONAL LAW AND THE APPLICABILITY, IF ANY, OF INTERNATIONAL LAW TO TRADITIONAL ESPIONAGE OR CYBER ESPIONAGE

A. Stuxnet

In various writings and various forums, Michael Schmitt has extensively explored the *jus ad bellum* aspects of cyber operations.[11] He has also extensively explored the *jus in bello* dimensions of cyber operations.[12] With respect to the *jus ad bellum* dimension of Stuxnet, the key issue is whether the Stuxnet virus directed against Iran's centrifuges constitutes a "use of force" prohibited by Article 2(4) of the UN Charter. Schmitt poses the applicable test as follows:

> That the term "use of force" encompasses resort to armed force by a state, especially force levied by the military is self-evident. Armed force thus includes kinetic force—dropping bombs, firing artillery, and so forth. It would be no less absurd to suggest that cyber operations that generate consequences analogous to those caused by kinetic force lie beyond the prohibition's reach, than to exclude other destructive non-kinetic actions, such as biological or radiological warfare. Accordingly, cyber operations that directly result (or are likely to result) in physical harm to individuals or tangible objects equate to armed force, and are therefore uses of force. For instance, those targeting an air traffic control system or a water treatment facility clearly endanger individuals and property.[13]

To my knowledge, Stuxnet did not threaten or cause physical harm to individuals, but as noted previously, it did cause physical harm to 1,000 centrifuges critical to the production of nuclear material by Iran. This would

---

11. See, e.g., Michael N. Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited*, 56 VILLANOVA LAW REVIEW 559 (2011). Another major article, which also explores the *jus in bello* dimensions of cyber operations, is Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885 (1999).

12. *See* Michael N. Schmitt, *Cyber Operations and the* Jus in Bello*: Key Issues*, *in* INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 89 (Raul A. "Pete" Pedrozo and Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies). *See also* Michael N. Schmitt, *Classification of Cyber Conflict*, 89 INTERNATIONAL LAW STUDIES 233 (2013).

13. Schmitt, *Cyber Operations and* the Jus ad Bellum *Revisited*, *supra* note 11, at 573.

seem to qualify as the kind of consequences to tangible property analogous to those caused by kinetic force suggested by Schmitt.

To be sure, Article 2(4)'s prohibition of the use of force applies by its terms only to "Members" of the United Nations.[14] This raises the issue of attribution, i.e., unless the use of the Stuxnet virus can be attributed to a State there is no violation of Article 2(4). As indicated earlier in this article, however, there is considerable evidence that the United States and Israel were behind the Stuxnet attacks.[15] For example, writing in the *New York Times* on June 1, 2010,[16] David Sanger reports that during his first months in office, President Obama "secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program."[17] The expanded first U.S. sustained use of cyber weapons that Sanger refers to had begun in the George W. Bush administration and was code named Olympic Games. It remained secret until the summer of 2010 when a programing error allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the virus gave it the nickname Stuxnet. According to Sanger, even after Stuxnet became public, President Obama decided to continue using it and after a few weeks of a series of attacks the result was that 1,000 of the 5,000 centrifuges Iran had spinning to purify uranium were temporarily taken out of commission.[18]

There is further evidence that the United States and Israel were behind the Stuxnet attacks.[19] First, the use of zero-day hacks (a zero-day hack exposes vulnerability in a piece of software that was previously unknown to the developer) demonstrates that this was likely the work of multiple programmers with a substantial budget. Indeed, some analysts have estimated that "it could have taken five to ten programmers upwards of six months

14. Article 2(4) of the UN Charter provides: "All Members shall refrain in their international relations from the use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

15. *See supra* notes 8 and 9 and accompanying text.

16. *See* Sanger, *supra* note 8.

17. *Id.*

18. *Id.*

19. *See* Jeremy Richard, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, 35 FORDHAM INTERNATIONAL LAW JOURNAL 842, 854 (2012).

to create Stuxnet."[20] Moreover, Stuxnet is a "highly specialized piece of malware" and "the narrow range of circumstances in which Stuxnet would deploy its payload makes it unlikely that Stuxnet had another purpose besides destroying nuclear centrifuges."[21] Additionally, the Israeli government's responses to news of the virus were highly suspicious. When Israeli officials were asked about their involvement in Stuxnet they "broke into wide smiles."[22] Also, a video played at the retirement party of former Israeli Defense Force Chief of General Staff Lieutenant General Gabi Ashkenazi featured references to Stuxnet as one of the general's operational successes, and, for its part, the United States has refused to deny involvement in Stuxnet.[23]

Assuming arguendo that Stuxnet constitutes a use of force in violation of Article 2(4) of the UN Charter,[24] the issue then arises whether it also constitutes an armed attack that would give Iran a right to exercise self-defense under Article 51 of the UN Charter.[25] At the time of this writing, the U.S. government has not publicly articulated a general position on cyber attacks and Articles 2(4) and 51.[26] There is some evidence that the United States has conflated the terms "use of force" under Article 2(4) and "armed attack" under Article 51, with the result that a cyber attack that constituted a use of force would also qualify as an armed attack, giving rise to a right of self-defense on the part of the State suffering the attack to engage in a military use of armed force.[27] But Michael Schmitt, along with

---

20. *Id.*

21. *Id.*

22. *Id.* at 856.

23. *Id.*

24. It is worth noting that in an email of August 14, 2012 to me, Michael Schmitt stated that in his opinion Stuxnet was a use of force under Article 2(4) (email on file with author).

25. Article 51 of the UN Charter reads as follows:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.

26. *See* Matthew Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421, 431 (2011).

27. For discussion, see *id.* at 431–37.

other commentators, rejects the idea that there is no difference between "a use of force" under Article 2(4) and an "armed attack" under Article 51. In Schmitt's view:

> The key text in Article 51, and the foundational concept of the customary law right of self-defense, is "armed attack." But for an armed attack, States enjoy no right to respond forcefully to a cyber operation directed against them, even if that operation amounts to an unlawful use of force. This dichotomy was intentional, for it comports with the general presumption permeating the Charter scheme against the use of force, especially unilateral action. In the *Nicaragua* case, the ICJ acknowledged the existence of this gap between the notions of use of force and armed attack when it recognized that there are "measures which do not constitute an armed attack but may nevertheless involve a use of force" and distinguished "the most grave forms of the use of force from other less grave forms." Recall that the court specifically excluded the supply of weapons and logistical support to rebels from the ambit of armed attack, but noted that such actions might constitute uses of force. Simply put, all armed attacks are uses of force, but not all uses of force qualify as armed attacks.[28]

Not all uses of force qualify as armed attacks, but some do, and the issue is whether Stuxnet qualifies as one of those that do. Schmitt has noted, correctly in my view, that "Article 51 restricts a state's right of self-defense to situations involving *armed* attack, a narrower category of act than Article 2(4)'s use of force."[29] Schmitt goes on to add: "Thus, faced with CNA [computer network attack] that does not occur in conjunction with, or as a prelude to, conventional military force, a state may only respond with force in self-defense if the CNA constituted armed force . . . intended to directly cause physical destruction or injury."[30] Under this standard, there would seem to be little doubt that Stuxnet qualified as an armed attack under Article 51. It should be noted, however, that Yoram Dinstein has argued that to qualify as an "armed attack" a cyber attack must produce "violent consequences."[31] In response to this argument, Matthew Waxman has suggested that

---

28. *See* Schmitt, *Cyber Operations and the* Jus ad Bellum *Revisited*, *supra* note 11, at 587.

29. *See* Schmitt, *Computer Network Attack and the Use of Force in International Law*, *supra* note 11, at 928.

30. *Id.* at 929.

31. *See* Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99, 103 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (Vol. 76, U.S. Naval War College International Law Studies) ("The

> [a] significant problem with this view is that in a world of heavy economic, political, military, and social dependence on information systems, the 'nonviolent' harms of cyber-attacks could easily dwarf the 'violent' ones. Consider, for example, a take-down of banking systems, causing cascades of financial panic, or the disabling of a power grid system for an extended period of time, causing massive economic disruption and public health emergencies.[32]

In his statement quoted above, Schmitt notes that the ICJ in the *Nicaragua* case supports the proposition that there is a gap between the notions of use of force and armed attack. It is important to note, however, that the U.S. government has emphatically rejected the Court's analysis in *Nicaragua*, as well as a similar analysis in the later ICJ decision in the *Oil Platforms* case.[33] Specifically, as to the *Nicaragua* decision, Abraham D. Sofaer, then-Legal Adviser of the U.S. Department of State, in a luncheon address jointly sponsored by the American Society of International Law and the Section of International Law and Practice,[34] sharply criticized the ICJ's comments on the right of self-defense, especially its narrow definition of the scope of the term "armed attack" to exclude "assistance to rebels in the form of the provision of weapons or logistical or other support."[35] In Sofaer's view, "[t]his ruling was without support in customary international law, or the practice of nations, which could not rationally be read to deprive a state of the right to defend itself against so serious a form of aggression."[36] Sofaer added that

> the ICJ's ruling concerning the use of force creates artificial distinctions and mechanical rules that are fundamentally inconsistent with the principled but flexible approach followed by the United States since the Charter's adoption. Its restrictive approach in defining "armed attack" could deprive states of the right of self-defense against the most common and dangerous forms of aggression in the world today.[37]

---

crux of the matter is not the medium at hand . . . but the violent consequences of action taken.").

32. See Waxman, *supra* note 26, at 436.

33. *See* Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161 (Nov. 6).

34. *See* Abraham D. Sofaer, *International Law and the Use of Force*, 82 AMERICAN SOCIETY OF INTERNATIONAL LAW PROCEEDINGS 420 (1988).

35. *Id.* at 425.

36. *Id.*

37. *Id.* at 426.

Writing in the *Yale Journal of International Law* in 2004,[38] William H. Taft, IV, then-Legal Adviser of the U.S. Department of State, was perhaps even more scathing in his criticism of the ICJ's comments on self-defense under international law in the *Oil Platforms* case than was Sofaer with respect to the Court's decision in *Nicaragua*. In *Oil Platforms*, Iran claimed that the United States had violated the "freedom of commerce" provision in the 1955 Treaty of Amity, Economic Relations and Consular Rights between the two countries by taking military action against Iranian offshore oil platforms in 1987 and 1988. Interestingly, the ICJ rejected Iran's claim, finding that the U.S. actions against the oil platforms did not disrupt commerce between the territories of Iran and the United States. In other words, the United States won the case. Nonetheless, the Court proceeded to devote "a substantial portion of its opinion to a consideration of whether the U.S. actions against the oil platforms qualified as self-defense under international law. The Court's statements concerning this issue were unnecessary to resolve the case and thus, in our domestic legal system, would be considered non-binding *dicta*."[39]

Parenthetically, I would suggest that Taft's characterization of the ICJ's statements as non-binding *dicta* was overly restrained. I would characterize the Court's discussion of whether the U.S. action against the oil platforms qualified as self-defense under international law as an outrageous abuse of the judicial process. Having decided that Iran had no claim under the Treaty of Amity with the United States, the Court had no legitimate reason to express its view on another argument the United States had made in response to Iran's claim. The Court was, after all, rendering a decision in a contentious case, not handing down an advisory opinion.[40]

Be that as it may, Taft argued that the Court's statements in the *Oil Platform* case concerning self-defense might be read as suggesting a number of limitations on the right of self-defense, namely:

- that an attack involving the use of deadly force by a State's regular armed forces on civilian or military targets is not an "armed attack"

38. William H. Taft, IV, *Self-Defense and the Oil Platforms Decision*, 29 YALE JOURNAL OF INTERNATIONAL LAW 295, 295 (2004) (emphasis in original).

39. *Id.*

40. In his article, Taft did note that five of the judges on the Court had expressly raised concerns about the majority's decision to address the issue of self-defense. *See id.* at 298. The five judges, all of whom wrote separate opinions, were Buergenthal, Higgins, Parra-Aranguren, Kooijmans and Owada.

> triggering the right of self-defense, unless the attack reaches some unspecified level of gravity;
> - that an attack must have been carried out with the intention of harming a specific State before that State can respond in self-defense; that self-defense may be directed only against targets of the attacking State that have been the subject of specific prior complaints by the defending State; and
> - that measures taken in self-defense must be proportional to the particular attack immediately preceding the defensive measures rather than proportional to the overall threat being addressed.[41]

Taft next stated categorically that "international law and practice do not support these limitations on the right of self-defense" and added, perhaps contrary to the fact, that "[t]he United States presumes that the Court did not intend to suggest these limitations."[42]

Interestingly, under either the Schmitt approach to armed attack,[43] the U.S. practice of conflating Article 2(4) and Article 51 or the ICJ's narrower definition of the scope of self-defense, there is a strong argument to be made that Stuxnet constituted both a use of force under Article 2(4) and an armed attack under Article 51. If so, it may seem odd that Iran's reaction to this cyber attack was so restrained, almost to the point of not acknowledging its existence. Indeed, although Iranian officials initially stated that a delay in its Bushehr nuclear power plant being operational was based on "technical reasons," it did not complain of it being the result of a cyber attack.[44] Later, Iran's President, Mahmoud Ahmadinejad, reported that malicious software had damaged the centrifuge facilities, but did not suggest that Iran had been the victim of a State-sponsored cyber attack, much less that it had been the victim of an armed attack and therefore had the right to respond with armed force in the exercise of its right of self-defense under Article 51.[45] It is unclear why Iran's reaction to the Stuxnet attack was so restrained,[46] but one result of this restraint is that there has been rela-

---

41. *Id.* at 299.

42. *Id.*

43. In his email to me of August 14, 2012, Michael Schmitt stated that it was his opinion that Stuxnet was both a use of force under Article 2(4) of the UN Charter and an armed attack under Article 51. *See supra* note 24.

44. *See* Brown, *supra* note 6.

45. *Id.*

46. In his article Gary Brown speculates about a variety of possible reasons for Iran's restraint. *See id.*

tively little reaction to Stuxnet in the world community and only a smattering of coverage in the media or legal literature.

B. International Law and Traditional Espionage

Several times during the "Cyber War and International Law" conference categorical comments were made that espionage is not prohibited by international law.[47] If one is considering traditional espionage, it is important to distinguish between espionage in war or armed conflict and peacetime espionage. Most scholarly writing on the relationship between espionage and international law concerns the law of war or armed conflict.[48] John Radsen has suggested:

> The rules of espionage in times of war, whether based on the Hague Regulations of 1907, the Geneva Conventions, the Protocol Additional to the Geneva Conventions, or other sources, are straightforward. A "scout," someone who stays in military uniform or sufficiently designates himself as a combatant, risks being caught behind enemy lines. If caught, this person should be dealt with as a prisoner of war because there is nothing treacherous or deceitful about his scouting or reconnaissance mission. But a spy, someone who does not wear a military uniform or a clear military designation, is not entitled to protection as a prisoner of war. His deceit can lead to severe punishment from the captors. Despite the potentially harsh penalties, the trial itself for the charge of espionage should follow standard procedures. Note, by the way, that if the spy returns to his military organization after his mission and is then captured in battle wearing a Soldier's uniform or designation, he cannot be punished for his prior act of spying. A spy therefore has a strong incentive to succeed in his spying mission and to return quickly to his military organization.[49]

The situation concerning espionage and international law outside of the law of war is much less straightforward. Indeed, Radsen quotes with approval as having contemporary relevance, a 1962 statement by Richard Falk: "[t]raditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether

47. *See, e.g.*, Dinstein, *supra* note 1, at 284.

48. *See* John Radsen, *The Unresolved Equation of Espionage and International Law*, 28 MICHIGAN JOURNAL OF INTERNATIONAL LAW 595, 601 (2007).

49. *Id.* at 602.

or contain a perfunctory paragraph that defines a spy and describes his hapless fate upon capture."[50]

Radsen goes on to report that the limited literature available on peacetime espionage can be divided into three groups:

> One group suggests peacetime espionage is legal (or not illegal) under international law. Another group suggests peacetime espionage is illegal under international law. A third group, straddled between the other two, maintains that peacetime espionage is neither legal nor illegal—perhaps, as Nietzsche would say, that it is beyond good and evil. In any event, the uncertainty in the literature supports my thesis that espionage is beyond international consensus.[51]

Of the three groups discussed by Radsen, the one that seems most convincing to me is the third: the group holding that espionage is neither legal nor illegal. In his discussion of the literature in the third group, Radsen quotes a writing by two former CIA officials, Daniel Silver, a former General Counsel, and Frederick Hitz, a former Inspector General.[52] In their writing, Silver and Hitz state that "[t]here is something almost oxymoronic about addressing the legality of espionage under international law."[53] Referring to the "ambiguous state of espionage under international law,"[54] they conclude that espionage is neither clearly condoned nor condemned under international law. Radsen adds by way of comment that:

> The rules and the ethics are situational. Countries are much less tolerant when espionage is committed against them than when they are committing it against friends and foes. Whether espionage is legal or illegal under international law, they are realistic about the fact that countries, for reasons of self-defense and for their own interests, are going to commit espionage in other countries. According to Silver and Hitz, that may explain why no treaties or conventions specifically prohibit espionage.[55]

---

50. *Id.* The cite to Falk is Richard Falk, *Foreword to* ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW, at v, v (Roland J. Stanger ed., 1962).

51. Radsen, *supra* note 48, at 602.

52. *Id.* at 606.

53. Daniel B. Silver (updated and revised by Frederick P. Hitz & J.E. Shreve Ariail), *Intelligence and Counterintelligence*, *in* NATIONAL SECURITY LAW 935, 965 (John Norton Moore & Robert F. Turner eds., 2d ed. 2005).

54. *Id.*

55. Radsen, *supra* note 48, at 606.

C. Cyber Espionage and International Law

Cyber espionage is a relatively new development that raises a basic question: Does cyber espionage differ from traditional espionage simply as a matter of degree, or is it an entirely new phenomenon that arguably poses new challenges for international law and practice? In addressing this issue, it is helpful to consider the workings of the new computer viruses with the nicknames Flame and Gauss.

The British Broadcasting Corporation first began reporting about the Flame virus in May 2012 after the Russian security firm Kaspersky Lab began investigating the matter.[56] The ITU had asked Kaspersky Lab to look into reports in April that computers belonging to the Iranian Oil Ministry and the Iranian National Oil Company had been hit with malware that was stealing and deleting information from their systems.

Flame is designed to monitor computer networks and send back intelligence to its creators.[57] It reportedly has the capacity to "activate computer microphones and cameras, log keyboard strokes, take screen shots, extract geolocation from images, and send and receive commands and data through Bluetooth wireless technology."[58] It also reportedly is more than twenty times larger than Stuxnet, and, most important, "whereas Stuxnet just had one purpose in life, Flame is a toolkit, so they can go after just about everything they can get their hands on."[59] Along the same lines, Kaspersky Lab's chief malware expert Vitaly Kamluk has reportedly described Flame as "basically an industrial vacuum cleaner for sensitive information."[60]

The virus appears to have a wide reach indeed, as more than six hundred specific targets were hit, ranging from individuals, businesses and academic institutions to government systems. Iran's National Computer Emergency Response Team posted a security alert stating that it believed Flame was responsible for "recent incidents of mass data loss" in the coun-

---

56. Reuven Cohen, *New Massive Cyber-Attack an "Industrial Vacuum Cleaner for Sensitive Information,"* FORBES (May 28, 2012), http://www.forbes.com/sites/reuvencohen/2012/05/28/new-massive-cyber-attack-an-industrial-vacuum-cleaner-for-sensitive-information/.

57. *See* Nakashima, Miller & Tate, *supra* note 10.

58. *Id.*

59. David Lee, *Flame: Massive Cyber-Attack Discovered, Researchers Say*, BBC NEWS (May 28, 2012), http://www.bbc.co.uk/news/technology-18238326.

60. *Id.*

try.[61] Among the countries affected by the virus are Iran, Israel, Sudan, Syria, Lebanon, Saudi Arabia and Egypt. Further instances of infected machines were detected in the United States, as well as in the United Kingdom and parts of Europe. Researchers, however, pointed out this did not necessarily mean these countries were targets, as "use of proxy servers can distort location data."[62]

Although the basic purposes behind Stuxnet and Flame appear to differ, the two viruses are similar in a number of ways, including the "names of mutually exclusive objects, the algorithm used to decrypt strings, and the similar approaches to file naming"; moreover, parts of the code are identical, especially the part responsible for the virus's distribution.[63] Alexander Gostev, chief security expert of Kaspersky Lab, described these similarities between the two viruses as "very strong evidence that Stuxnet/Duqu and Flame cyber-weapons are connected."[64]

A recent *Washington Post* article directly attributed Flame to the United States and Israel, stating that they developed the virus to gather intelligence "in preparation for cyber-sabotage aimed at slowing Iran's ability to develop a nuclear weapon."[65] Both American and Israel officials, however, have denied the *Washington Post*'s claim, and the evidence is conflicting.[66]

Kaspersky Lab recently discovered the fourth allegedly State-sponsored computer virus to surface in the Middle East in the past three years, apparently aimed at computers in Lebanon.[67] According to Kaspersky Lab, the virus appeared to have been written by the same programmers who created Flame and may be linked to Stuxnet. This latest virus, nicknamed Gauss after a name found on its code, has been detected on 2,500 computers, most of them in Lebanon. The firm said its purpose appeared to be to acquire

---

61. *Id.*

62. *Id.*

63. *See Resource 207: Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected,* KASPERSKY LAB (June 11, 2012), http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected.

64. *Id.*

65. *See* Nakashima, Miller & Tate, *supra* note 10.

66. *See* Sanger, *supra* note 8 (U.S. officials denying Flame was part of Olympic Games); Hayley Tsukayama, *Flame Cyberweapon Written Using Gamer Code, Report Says*, WASHINGTON POST (May 31, 2012), http://articles.washingtonpost.com/2012-05-31/business /35456034_1_stuxnet-flame-virus-skywiper%20 (Israel's denial of involvement with Flame).

67. *See* Nicole Perlroth, *Computer Virus Is Aimed at Banks in Lebanon, Security Firm Says*, NEW YORK TIMES, Aug. 10, 2012, at A4.

"logins for email and instant messaging accounts, social networks and, notably, accounts at certain banks—a function more typically found in malicious programs used by profit-seeking cybercriminals."[68]

Lebanese experts reportedly said that an American cyber espionage campaign directed at Lebanon's banking system was plausible, given U.S. concerns that the country's banks are being used as a financial conduit for the Syrian government and for Hezbollah, the Lebanese militant group and political party. Researchers at Kaspersky Lab stated they were confident that Gauss was the work of the same hands as Flame, because the viruses were written in the same language (known as C++) on the same platform and shared some code and features.[69]

At a minimum, it is clear that computer viruses such as Flame and Gauss constitute a method of espionage whose efficiency greatly exceeds that of traditional espionage. If Flame, for example, truly is "basically an industrial vacuum cleaner for sensitive information," it raises an unprecedented threat to the national security interests of targeted States. It has been argued that only Russia, China, Israel and the United States have the capability of engaging in such sophisticated espionage.[70] And there appears little doubt that the United States has an extraordinary capacity to engage in such espionage. Richard Clarke, however, who served three presidents as a counterterrorism czar, has argued that, although the United States has developed the capability to conduct an offensive cyber war, it has virtually no *defense* against the cyber attacks he says are targeting it now, and those that will be in the future.[71]

Clarke argues further that China in particular is engaged in cyber espionage that greatly threatens U.S. national security and goes so far as to claim that "[e]very major company in the United States has already been penetrated by China."[72] As an example, Clarke argues that the manufacturer of the F-35, the U.S. next generation fighter bomber, has been penetrated and

---

68. *Id.*

69. *Id.*

70. *See* Stephen Dockerty, *Virus Plunges Lebanon into Cyber War,* THE DAILY STAR (Aug. 11, 2012), http://www.dailystar.com.lb/News/Local-News/2012/Aug-11/184234-virus-plunges-lebanon-into-cyber-war.ashx#axzz2GqgfT6Pm.

71. This is the basic theme of RICHARD A. CLARKE & ROBERT KNAKE, CYBER WAR (2010). *See also* Ron Rosenbaum, *Richard Clarke on Who Was Behind the Stuxnet Attack*, SMITHSONIAN, Apr. 2012, at 12, *available at* http://www.smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html (in which the author interviews Clarke).

72. *Id.* at 17.

the F-35 details stolen. He also contends that our supply chain of chips, routers and hardware imported from China and other foreign suppliers may have been implanted with "logic bombs," trapdoors and "Trojan Horses," all ready to be activated on command. As a result, Clarke is reported as saying:

> My greatest fear is that, rather than having a cyber-Pearl Harbor event, we will instead have this death of a thousand cuts. Where we lose our competitiveness by having all of our research and development stolen by the Chinese and we never really see the single event that makes us do something about it.[73]

Clarke's concerns go way beyond the cost of lost intellectual property, and focus on the possible loss of military power. He envisions a confrontation, like the one in 1996 when President Clinton rushed two carrier battle groups to the Taiwan Strait to warn China against an invasion of Taiwan. This time, he suggests,

> we might be forced to give up playing such a role for fear that our carrier group defenses could be blinded and paralyzed by Chinese cyberintervention. (He cites a recent war game published in an influential military strategy journal called *Orbis* "How the U.S. Lost the Naval War of 2015").[74]

It is arguable that the use of cyber viruses with the efficiency of Flame or Gauss for espionage purposes constitutes a violation of current international law. As indicated previously,[75] Iran's National Computer Emergency Response team posted a security alert stating that it believed that Flame was responsible for recent incidents of "mass data loss" in the country. If one views data as a form of property, indeed a very important form of property in the modern world, a mass loss of data could constitute an armed attack. Also, if Clarke's allegation that China has penetrated by cyber means every major company in the United States, with the result that major military assets like advanced fighter jets and aircraft carriers have been compromised or even rendered dysfunctional is true, this raises the issue of the need for anticipatory self-defense against a great threat to U.S. national

73. *Id.*
74. *Id.*
75. *See* Lee, *supra* note 59 and accompanying text.

security—"perhaps the most controversial question in relation to the right of self-defence."[76]

To be sure, Christopher Greenwood, a judge on the ICJ, has stated that claims that cyber attacks should be considered armed attacks should be "treated with considerable caution."[77] Judge Greenwood suggests:

> The planting of a virus or the use of other computer techniques to undermine, for example, the computer systems regulating a State's financial system or immigration controls is difficult to see as an armed attack. Although the consequences of such conduct may be very serious, it seems closer to the concept of economic coercion. On the one hand, if such action were used to produce results similar to those which could otherwise be achieved only by the use of armed force, for example, causing aircraft to crash or dams to open and flood areas of a State's territory, then the argument that such action should be treated as a form of armed attack is more plausible.[78]

Judge Greenwood's words of "considerable caution" should be taken seriously. In his article, however, there is no discussion of the four advanced computer viruses, which arguably introduce new complexities to the multifaceted debate over the scope of the self-defense concept. Ideally, it should be possible to convene a global international conference to consider whether the advent of cyber attacks has created a need for revision of the *jus ad bellum* or the *jus in bello*. But as I have tried to demonstrate in another forum, it has proven very difficult in today's environment for an international conference to conclude a global treaty to resolve challenges in the most important areas of international relations.[79] In the area of the law of armed conflict, there is considerable concern that any major treaty that would result from a global conference would undermine rather than improve the current law.[80]

---

76. *See* Christopher Greenwood, *Self-Defence*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW ¶ 41 (2011), http://www.mpepil.com/sample_article?id=/epil/entries/law-9780199231690-e401&recno=2&.

77. *Id.* ¶ 14.

78. *Id.*

79. *See* MURPHY, *supra* note 5. The five topical areas covered are the maintenance of international peace and security, the law of armed conflict, arms control and disarmament, human rights and international environmental issues.

80. *See id.* at 161–80. *See also* Jean-Philippe Lavoyer, *International Humanitarian Law: Should It be Reaffirmed, Clarified or Developed?*, *in* ISSUES IN INTERNATIONAL LAW AND MILITARY OPERATIONS 287 (Richard B. Jacques ed., 2006) (Vol. 80, U.S. Naval War College

The validity of this concern is demonstrated by recent efforts in international forums to regulate the cyber field, including the possibility of cyber war. Indeed, as suggested in the introduction to this article, these efforts arguably constitute a use of the international legal process in a way that threatens U.S. and other Western States' vital interests. It is to this important issue that the next section of this article turns.

III. EFFORTS TO USE THE INTERNATIONAL LEGAL PROCESS TO REGULATE CYBER ACTIVITIES, INCLUDING CYBER WAR, IN A WAY THAT THREATENS U.S. AND OTHER WESTERN STATES' VITAL INTERESTS

As this article is being written, the *Financial Times* features a full page article on the UN World Conference on International Telecommunications, scheduled to be held in Dubai in December 2012 and sponsored by the ITU, a specialized agency of the United Nations.[81] Although, technically, the conference is supposed to focus on international agreements governing telecommunications, some proposals are expected to stretch broadly into the controversial issue of governance of the Internet. According to the *Financial Times*:

> The battle is already being fought behind closed doors at the International Telecommunications Union. . . . Western nations—such as the US and the EU—in particular do not want to give the ITU extra authority that could indirectly benefit authoritarian regimes in the Middle East, eastern Europe and Asia. They are accused of seeing an opportunity to enhance their ability to control the web and crack down on political dissidents.
>
> "If new governance rules had been set to tighten the control of the web a few years ago we would not have had an Arab spring," says one senior EU diplomat. "The internet must be left free and untouched, the less we tinker with it the better."[82]

There can be little doubt about the validity of the senior EU diplomat's observation that if new governance rules had been in place to tighten control of the web at the time of the Arab spring uprising in the Middle East, it

---

International Law Studies). For a comment on Lavoyer's presentation, see John F. Murphy, *Enforcing the Law*, *in id.* at 311.

81. *See* Daniel Thomas, Richard Waters & James Fontanella-Klan, *The Internet: Command and Control*, FINANCIAL TIMES (London), Aug. 28, 2012, at 5.

82. *Id.*

would never have taken place, or at a minimum would not have enjoyed the success it did. His observation also illustrates an example of a possible connection between efforts to gain control of the Internet and cyber war. It will be remembered that the Arab Spring led to initial violence in Egypt, a civil war in Libya that, with the aid of NATO air coverage, resulted in a regime change, and to the extreme violence in Syria. A major goal of Russia and China—the leaders in the effort to issue regulations that would put limits on use of the Internet—is to ensure that they will not be subject to uprisings like the Arab Spring that result in regime change. Their hard line against Western efforts in the UN Security Council to impose stringent economic sanctions or other forceful measures against the Assad government in Syria in the name of the responsibility to protect illustrates how far they are opposed to the entire concept of forceful regime change.[83]

Russia and China have been pressing their efforts to achieve international regulation of the Internet for some time now. For example, by letter of September 12, 2011, Russia, China, Tajikistan and Uzbekistan, transmitted an International Code of Conduct for Information Security to the UN Secretary-General.[84] The United States and other countries' responses to this proposal have been lukewarm at best, and the United States has been consistent in its resistance to proposals calling for control of the Internet passing to a UN agency.[85] For example, Terry Kramer, the U.S. Ambassador to the Dubai conference, has been reported as saying that

> [t]he US is concerned that proposals by some other governments could lead to greater regulatory burdens being placed on the international telecom sector, or perhaps even extended to the internet sector. The United States also believes that existing multi-stakeholder institutions, incorporating industry and civil society, have functioned effectively and will continue to ensure the health and growth of the internet and all its benefits.[86]

---

83. For discussion of the Arab spring and the responsibility to protect, see John F. Murphy, *Responsibility to Protect (R2P) Comes of Age? A Sceptic's View*, 18 ILSA JOURNAL OF INTERNATIONAL & COMPARATIVE LAW 413 (2012).

84. For text of the code, see Letter dated September 12, 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, Annex, U.N. DOC. A/66/359 (Sept. 14, 2011).

85. *See* Leo Kelion, *US Resists Control of Internet Passing to UN Agency*, BBC NEWS TECHNOLOGY (Aug. 3, 2012, 9:13 PM), http://www.bbc.co.uk/news/technology-19106420.

86. *Id.*

Similarly, according to a recently released document, "[t]he United States will oppose efforts to broaden the scope of the ITRs (International Telecommunication Regulations) to empower any censorship of content or impede the free flow of information and ideas."[87]

In sharp contrast, during a meeting in 2011 between then Russian Prime Minister Vladimir Putin and ITU Secretary-General Dr. Hamadoun Touré, Putin reportedly told Touré that Russia was keen on the idea of "establishing international control over the Internet using the monitoring and supervisory capability of the International Telecommunications Union."[88] It is hardly surprising that countries like China and Iran would support Putin's proposal.[89] But it is at least disappointing to learn that democratic countries like Brazil and India reportedly "share the belief that the Geneva-based UN agency the International Telecommunications Union (ITU) would do a better job if put in charge of international cyber-security, data privacy, technical standards and the global web address system."[90]

In response to the Russian challenge, "at least within the U.S., condemnation of the ITU's dangerously amateurish behavior has been universal. Republican and Democrats, Congress, the White House and the FCC [Federal Communications Commission], along with major industry representatives, consumer advocates, and engineering groups including the highly-respected and international Internet Society, have all raised alarms over both the content and the process of upcoming negotiations."[91] For its part, on April 19, 2012, the U.S. House of Representatives received a draft resolution whereby it was

> the sense of the House of Representatives that if a resolution calling for endorsement of the proposed international code of conduct for information security or a resolution inconsistent with the principles above comes up for a vote in the United Nations General Assembly or other international organization, the Permanent Representative of the United

87. *See* Larry Downes, *Why is the UN Trying to Take over the Internet?,* FORBES (Aug. 9, 2012), http://www.forbes.com/sites/larrydownes/2012/08/09/why-the-un-is-trying-to-take-over-the-internet/.

88. *Id.*

89. *Id.*

90. *See Russia Calls for Internet Revolution*, RT QUESTION MORE (May 28, 2012), http://rt.com/news/itu-internet-revolution-russia-386/.

91. *See* Downes, *supra* note 87.

> States to the United Nations or the United States representative to such other international organization should oppose such a resolution.[92]

At this writing, the draft resolution has been referred to the House Committee on Foreign Affairs but no further action has been taken on it.

It remains to be seen what will happen in December at the conference in Dubai. One possibility is that the meeting could prove inconclusive. Although each of the 193 countries expected to attend the meeting will have a vote, and the United States and like-minded countries could therefore be outvoted, Dr. Toure' reportedly has insisted that there will be no votes at the conference and no proposal will be passed without consensus.[93] It may be impossible to reach consensus, however, on the controversial governance proposals, and if so, there is a good chance that action on them will be postponed at least for a year.[94]

It remains to be considered whether it would be a good idea to try to reach an agreement on the terms of an arms control treaty on cyber weapons. In its July 1, 2010 issue, the *Economist* noted that Russia had engaged in "longstanding calls for a treaty."[95] Surprisingly, the *Economist* also reported that General Keith Alexander, who heads U.S. Cyber Command, had welcomed the Russian initiative as a "starting point for international debate."[96] The report is surprising because the United States has resisted Russian calls for an arms control treaty on cyber war,[97] and there is no indication that U.S. policy on this subject has changed.

There are several possible reasons for the U.S. resistance to Russian calls for a treaty on cyber war. For one thing, nation-States have differing views on what constitutes cyber-warfare. Most advanced democracies see cyber attacks as "an assault on the computer infrastructure that underlies power, telecommunications, transportation and financial systems."[98] Russia, however, prefers to call cyber warfare an "information war" and has introduced a resolution in the United Nations every year since 1998 calling for a

---

92. H. R. Res. 628, 112th Cong. (2012).

93. *See* Thomas, Waters & Fontanella-Khan, *supra* note 81.

94. *Id.*

95. *See Cyberwar: It is Time for Countries to Start Talking about Arms Control on the Internet*, ECONOMIST, July 3, 2010, at 11, *available at* http://www.economist.com/node/16481504.

96. *Id.*

97. *See e.g.*, Tom Gjelten, *Seeing the Internet as an "Information Weapon*," NPR (Sept. 23, 2010), http://www.npr.org/templates/story/story.php?storyId=130052701.

98. *Id.*

treaty outlawing "information terrorism."[99] According to Russian Defense official Sergei Korotkov, "anytime a government promotes ideas on the Internet with the goal of subverting another country's government—even in the name of democratic reform—it should qualify as 'aggression.'"[100]

In its article on "Cyberwar," the *Economist* suggests that the United States has

> resisted weapons treaties for cyberspace for fear that they could lead to rigid global regulation of the internet, undermining the dominance of American internet companies, stifling innovation and restricting the openness that underpins the net. Perhaps America also fears that its own cyberwar effort has the most to lose if its well-regarded cyberspies and cyber-warriors are reined in.[101]

At the same time, the *Economist* acknowledges another, perhaps more compelling, reason for U.S. hesitation: "a START-style treaty may prove impossible to negotiate. Nuclear warheads can be counted and missiles tracked. Cyber-weapons are more like biological agents; they can be made just about anywhere."[102]

As noted by Michael Schmitt in 1999, military thinkers devised and developed a term—information operations (IO)—anticipating this "new category of warfare" that grows from the Internet's interconnectivity and other new forms of communications.[103] In the same year, the U.S. Department of Defense Office of General Counsel rejected calls for IO-specific rules as "premature", arguing, *inter alia*, that in regulating IO via the law of war, the "process of extrapolation appears to be reasonably predictable."[104] Perhaps more surprisingly, in light of its generally favoring the development of new norms in the law of war, in 2003, the International Committee for the Red Cross expressed the view that "the existing legal framework is on the whole

---

99. *Id.*

100. *Id.*

101. *See Cyberwar*, *supra* note *95*.

102. *Id.*

103. *See* Schmitt, *Computer Network Attack and the Use of Force in International Law*, *supra* note 11, at 890.

104. Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (2d ed. Nov. 1999), *reprinted in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 31, at 459, 475 ("There seems to be no particularly good reason for the United States to support negotiations for new treaty operations in most of the areas of international law that are directly relevant to information operations." *Id.* at 522.).

adequate to deal with present day international armed conflicts."[105] Writing in 2007, Duncan Hollis stated that "[a] majority of military thinkers agree, arguing in favor of an analogy approach or decrying the possibility of IO-specific rules as premature or unrealistic."[106] It appears that a majority of military thinkers and U.S. government officials are still opposed to the negotiation of a new international convention on cyber war.[107] There is greater support for the negotiation of such a convention among civilian academic writers.[108] In my view, the arguments in favor of this view have considerable cogency and might well carry the day if the circumstances of today's world were more favorable to this possibility.[109] But they are not.

I have already noted the difficulty involved in trying to conclude a global treaty to resolve challenges in the most important areas of international relations, including the law of armed conflict.[110] The difficulties and the risks may be especially severe in the areas of maintenance of interna-

---

105. INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS 4 (2003), *available at* http://www.icrc.org/eng/assets/files/other/ihlcontemp_armedconflicts_final_ang. pdf.

106. See Duncan B. Hollis, *Why States Need An International Law For Information Operations*, 11 LEWIS & CLARK LAW REVIEW 1023, 1038–39 n.65 (2007).

107. Recently, Steven G. Bradley, who served for almost five years as the head of the Office of Legal Counsel in the Department of Justice during the George W. Bush administration, and had "occasion to advise on cybersecurity issues" during his tenure, stated categorically that:

> In the face of this lack of clarity on key questions, some advocate for the negotiation of a new international convention on cyberwar—perhaps a kind of arms control agreement for cyber weapons. I believe there is no foreseeable prospect that this will happen. Instead, the outlines of accepted norms and limitations in this area will develop through the practice of leading nations. And the policy decisions made by the United States in response to particular events will have great influence in shaping those international norms. I think that's the way we should want it to work.

Steven G. Bradbury, *The Developing Legal Framework for Defensive and Offensive Operations*, 2 HARVARD NATIONAL SECURITY JOURNAL 591, 611 (2011).

108. *See, e.g.*, Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 JOURNAL OF THE NATIONAL ASSOCIATION OF ADMINISTRATIVE LAW JUDICIARY 602 (2011) (who favors the negotiation of such a convention, but also cites and discusses both writers who favor and those who oppose the negotiation of such a convention).

109. In particular, I find the arguments of Hollis, *supra* note 106, to be quite persuasive. Hollis, currently a professor at Temple University School of Law, spent six years in the Office of the Legal Adviser, U.S. Department of State, before going into academia.

110. *See supra* notes 79 and 80 and associated textual discussion.

tional peace and security[111] and the law of armed conflict.[112] This is because the world has become increasingly hostile to the values and interests of Western democracies and nation-States increasingly prone to negotiate on a zero-sum basis.[113] Russia and China, States that have progressively assumed leadership roles in this new environment, are dictatorships hostile to the United States in particular, and so-called emerging powers such as India, Brazil and Turkey are "not ready for prime time."[114] In such an environment, the negotiation of an international convention on cyber war would indeed seem "premature."

If it is "premature" to try to negotiate an international convention on cyber war, are there other steps that might be taken to mitigate some of the problems posed by cyber threats? It is worth noting that the *Economist* writing in 2010 noted the difficulties of negotiating "a START-style treaty"[115] and suggested instead that "countries should agree on more modest accords, or even just informal 'rules of the road' that would raise the political cost of cyber-attacks."[116]

The *Economist*'s reference to informal rules of the road raises the controversial issue of so-called "soft law." The term "soft law" is controversial because various commentators, including this one, believe that use of the term creates confusion, especially because there is no agreement on what the term "soft law" means, and therefore is unhelpful.[117] One definition of soft law would include non-binding guidelines or even rules of the road. In some instances, especially in the fields of human rights or international environmental law, such guidelines are a step toward the eventual conclusion of a binding treaty. But, as I have stated elsewhere, use of the term soft law is "especially unfortunate when, as is arguably increasingly the case, legally nonbinding international instruments are utilized not as part of the process of making international law but rather as an alternative to it . . . because of the perception that application of legally binding international norms would not be appropriate under the circumstances."[118]

---

111. *See* MURPHY, *supra* note 5, at 103–60.

112. *Id.* at 161–80.

113. *See especially* IAN BREMMER, EVERY NATION FOR ITSELF (2012).

114. *See* Fareed Zakaria, *A Post-American World in Progress: Why Emerging Powers Didn't Lead in 2011 and Won't in the Coming Year*, TIME, Jan. 9, 2012, at 17.

115. *See Cyberwar, supra* note 95.

116. *Id.*

117. For my views on this controversy, see MURPHY, *supra* note 5, at 20–23.

118. *Id.* at 22–23.

In addition to recognizing the possibility of establishing "a set of non-legally binding norms with the expectation that international legal rules will emerge from them in time,"[119] Duncan Hollis has suggested that

> the path to creating international law need not always occupy the global stage. Perhaps the starting point for ILIO [international law for information operations], like the law of war itself, might best lie in one or more individual nation-states producing a set of self-governing rules for their own IO. Or, a group of interested states might decide to articulate an ILIO among themselves, as the Council of Europe did for Cybercrime . . . .[120]

However States may decide to approach the problems posed by cyber war, they will have to cope with the special challenges created by the increasingly global operations of terrorist groups like Al Qaeda. We turn to a consideration of these challenges in the next section of this article.

IV. TERRORISM AND CYBER WAR

The literature on terrorism is vast, but there is no need discuss it in this article. Rather, for present purposes, the focus will be on what has been called the "new terrorism."[121] The quintessential example of a group engaged in the new terrorism is Al Qaeda, and the quintessential example of a new terrorism act is the horrific attacks of September 11, 2001. With respect to the old terrorism, the conventional wisdom suggested that terrorists had little interest in killing large numbers of people. The perception was that large scale killings would undermine their efforts to gain sympathy for their cause, which was usually to overthrow the government of a particular country (e.g., Germany or Italy). In sharp contrast, an especially disquieting aspect of the new terrorism is the increased willingness of terrorists to kill large numbers of people. For example, the terrorist attacks in the United States on September 11, 2001 killed 2,973 people; in Madrid on March 11, 2004, attacks killed 191 and wounded 2,050; and in the bombings in the Mumbai (Bombay) train system on July 11, 2006, they killed 209

119. *See* Hollis, *supra* note 106, at 1059.

120. *Id.*

121. *See, e.g.*, John F, Murphy, *Challenges of the "New Terrorism," in* ROUTLEDGE HANDBOOK OF INTERNATIONAL LAW 281, 283–86 (David Armstrong ed., 2009).

and injured more than 700.[122] Jeffrey D. Simon has aptly pinpointed a major cause of the radical change in attitude:

> Al Qaeda . . . is representative of the emergence of the religious-inspired terrorist groups that have become the predominate form of terrorism in recent years. One of the key differences between religious-inspired terrorists and politically motivated ones is that the religious-inspired terrorists have fewer constraints in their minds about killing large numbers of people. All nonbelievers are viewed as the enemy, and the religious terrorists are less concerned than political terrorists about a possible backlash from their supporters if they kill large numbers of innocent people. The goal of the religious terrorist is transformation of all society to their religious beliefs, and they believe that killing infidels or nonbelievers will result in their being rewarded in the afterlife. Bin Laden and Al Qaeda's goal was to drive U.S. and Western influences out of the Middle East and help bring to power radical Islamic regimes around the world. In February 1998, bin Laden and allied groups under the name "World Islamic Front for Jihad Against the Jews and the Crusaders" issued a fatwa, which is a Muslim religious order, stating that it was the religious duty of all Muslims to wage a war on U.S. citizens, military and civilian, anywhere in the world.[123]

Another facet of the new terrorism is the extraordinary extent to which terrorists have developed global networks. A recent study finds that Al Qaeda operates in a network that spans roughly one hundred countries, including the United States.[124] While that network has weakened severely in recent years with the assassination or capture of key Al Qaeda leaders such as Osama bin Laden, the Al Qaeda organization has simultaneously gained many new militants to its cause through a "terror by franchise" approach.[125] That is, while the jihadi threat has been suppressed in some countries (e.g., Saudi Arabia and Indonesia) it is increasing in places in North Africa and Lebanon. Groups inspired by Al Qaeda have in turn established links with a new breed of home-grown terrorist. The problem is especially acute in

---

122. *See* BETH VAN SCHAACK & RONALD C. SLYE, INTERNATIONAL CRIMINAL LAW AND ITS ENFORCEMENT 615 (2d ed. 2010).

123. Jeffrey D. Simon, *The Global Terrorist Threat,* 82 PHI KAPPA PHI FORUM 10, 11 (2002).

124. Jayshree Bajoria & Greg Bruno, *al-Qaeda (a.k.a. al-Qaida, al-Qa'ida),* http://www.cfr. org/publication/9126/ (last updated June 6, 2012).

125. *See, e.g.*, Farhan Bokhari & Stephan Fidler, *Rivalries Rife in Lair of Leaders*, FINANCIAL TIMES (London), July 5, 2007, at 5.

the United Kingdom, where radicalized British Muslims have established links with Al Qaeda and Taliban-sponsored training camps in Pakistan.[126] In continental Europe, home grown terrorists have established links with radical cells in North Africa.

The concern that terrorists may resort to the use of weapons of mass destruction—nuclear, chemical, or biological—is long standing.[127] Since September 11, however, this concern has been greatly heightened. Moreover, Osama bin Laden and Al Qaeda made plain on numerous occasions their desire to obtain weapons of mass destruction, especially nuclear weapons, and their use of civilian aircraft on September 11 and their effective employment of the Internet since then have demonstrated their technological competence. Their proficiency with computers has led one commentator to suggest that they now have the capacity for hijacking satellites: "Capturing signals beamed from outer space [it is alleged] terrorists could devastate the communications industry, shut down power grids, and paralyze the ability of developed countries to defend themselves."[128]

Interestingly, there appears currently to be a tendency to play down the risk of terrorists being engaged in a cyber war, on the ground that today's cyber attacks are so sophisticated that they require a State government to carry out rather than individual terrorists or terrorist organizations operating on their own.[129] This view may be too complacent, however.[130] Certain-

126. *See* Stephen Fidler, *Radicalising Wave Crosses the Atlantic*, FINANCIAL TIMES (London), July 5, 2007, at 5.

127. *See* Brian M. Jenkins & Alfred P. Rubin, *New Vulnerabilities and the Acquisition of New Weapons by Nongovernmental Groups*, *in* LEGAL ASPECTS OF INTERNATIONAL TERRORISM 221 (Alone E. Evans & John F. Murphy eds., 1978).

128. *See* Lawrence Wright, *The Terror Web*, NEW YORKER, Aug. 2, 2004, at 40, 50, *available at* http://www.newyorker.com/archive/2004/08/02/040802fa_fact.

129. *See e.g.*, Richard, *supra* note 19, at 854 (where the author notes that the sophistication of the Stuxnet virus is so great that "it could have taken five to ten programmers upwards of six months to create Stuxnet" and therefore it is likely that a government or governments is behind it rather than individual hackers). *See also* Charles J. Dunlap Jr., *Meeting the Challenge of Cyberterrorism: Defining the Military Role in a Democracy, in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW, *supra* note 31, at 353, 359 (arguing that the absence of any catastrophic events caused by IO demonstrates that IO may be more difficult to accomplish than theorists realize, but conceding that IO still poses a threat in certain contexts, such a IO's capacity to steal identities).

130. For example, during its 2006 armed conflict with Israel, Hezbollah, which the United States and Israel have labeled a terrorist organization, reportedly engaged in cyber war against Israel. According to the report,

> While fighting raged in the towns and hills of southern Lebanon, Hizbullah launched an all-out assault on Israeli civilian and military communications networks. Hizbullah hackers

ly the computer capability demonstrated by Al Qaeda is sufficient to allow it to be intensively involved in cyber espionage, and as to mounting a cyber attack that would result in a large number of deaths and major property damage, there is an increasing risk that State adversaries of the United States and other Western democracies might give the support to terrorist groups necessary to allow them to engage in such a cyber attack. For example, Iran might give such support to Al Qaeda, and certain elements of the Pakistani government might do the same with the Taliban and Al Qaeda.

As is well known, a major challenge in defending against a cyber attack is the problem of attribution, i.e., determining where the attack came from and who or what engaged in it. The problem of attribution is greatly compounded when a cyber attack is engaged in by a terrorist organization like Al Qaeda that is globally networked in over a hundred countries. In considering the feasibility of developing a customary ILIO, Hollis argues that

> attribution issues may make it difficult to ever discern state practice in IO. IO's strength often lies in its anonymity and secrecy—victims of IO may not know that they have been subjected to it, let alone who is responsible (although constantly changing technology ensures that this will not always be the case).[131]

Hollis also cautions that "it can take years or decades for state practice to coalesce into customary international law."[132] Moreover, it should be noted, dramatic changes in the nature of international relations have made the process of creating customary international law particularly problematic.[133]

> shut down Israeli phone systems, electric grids, and IT systems periodically throughout the war. At the same time, they hacked into phone lines and eavesdropped on Israeli conversations, including those of Israeli soldiers, who, in many instances, gave away important tactical information on phone calls home. The hackers even cracked encrypted Israeli military communications, providing the militants with information on Israeli movements and intentions. Through electronic warfare, Hizbullah made life even more difficult in northern Israel and, at the same time, gained valuable, tactical intelligence on its enemies.

Andrew Chadwick, *The 2006 Lebanon War: A Short History, Part II*, SMALL WARS JOURNAL 5 (Sept. 12, 2012), http://smallwarsjournal.com/jrnl/art/the-2006-lebanon-war-a-short-history-part-ii (citation omitted).

131. *See* Hollis, *supra* note 106, at 1054.

132. *Id.*

133. For discussion and citations, see MURPHY, *supra* note 5, at 16–19.

It is at least arguable that the threats to States are no longer primarily from other States, but from non-State actors. If this is the case, Hollis asks, "do we serve international peace and security by imposing so many restrictions on how states use IO against non-state actors."[134] Answering his question in the negative, Hollis continues:

> For example, rather than seeing ILIO as essentially a question of restricting what States do to one another, ILIO could establish rules enabling states to better meet the challenges posed by non-state actors, particularly those bent on global terror. In the language of economists, ILIO may reduce the transaction costs that states face in combating transnational terrorism. The current system—which might prohibit a state from responding to an al-Qaeda attack from Pakistan directly or immediately, requiring it instead to ask Pakistan for assistance—is not terribly efficient and may have high costs for the victim state's safety and security. In its place, ILIO offers an opportunity for states to acknowledge their collective interest in combating non-state terrorist actors as a threat to the state system itself, and to devise cooperative mechanisms that increase the efficiency of such efforts. This might involve, for example, states such as Pakistan consenting to suspend the non-intervention principle in certain pre-agreed circumstances and allowing injured states to respond immediately and directly to IO generated from their territory (i.e., to conduct an active defense to CNA). Or, perhaps states could establish a program where a state sends information officers to other states who can approve IO methods that target or transit the sending state's territory. There is already some precedent for this in the maritime context, through the practice of "shiprider" agreements, in which a foreign state agrees that one of its officials may serve abroad a U.S. ship and authorize it to conduct law enforcement activities against ships of that foreign state and even within the foreign state's territorial seas.[135]

Hollis's remarks are intriguing. They posit, correctly in my view, that even adversarial States, for example, Russia and the United States, may have a common interest in agreeing upon rules, perhaps informal in nature, that allow them to cooperate in employing IO in combating global terrorism. The proposition that cooperation between Pakistan and the United States in combating IO by terrorists is possible may be a bit more problematic in light of evidence of Pakistan's Inter-Services Intelligence Directorate assisting the Taliban in Afghanistan in their use of improvised explo-

134. Hollis, *supra* note 106, at 1055.
135. *Id.* at 1055–56.

sive devices against members of the Afghanistan government and coalition forces.[136] But even in this case, Pakistan might be more amenable to cooperating with the United States in using IO to response to Taliban or Al Qaeda attacks launched from Pakistan into Afghanistan than it has been with respect to drone attacks launched by the United States into Pakistan against the Taliban or Al Qaeda.

In any event, at a minimum efforts to reach informal "rules of the road" regarding the use of IO against global terrorism would seem warranted. There seems little doubt that the greatest national security threat facing the United States and its allies in the coming years is asymmetric warfare, of which cyber warfare is a prime example.

V. CONCLUSION

To answer the question posed in the title of this article, i.e., whether the international legal process may constitute a threat to U.S. vital interests in the area of cyber war and international law, the answer is it may unless the United States and its allies resist efforts by Russia and other like-minded States to establish international regulation of the Internet that would benefit authoritarian regimes and endanger basic values such as freedom of speech and privacy. Similar efforts by Russia in particular to conclude a treaty on cyber war that could undermine the United States and other Western States' national security must also be resisted. At the same time, at least with respect to cyber war and international law, it may be desirable to engage in more modest steps, such as considering possible non-binding guidelines, either as a first step toward an eventual binding treaty or as a substitute for such a treaty.

Although the conventional wisdom that holds that traditional espionage is not regulated by international law, with the exception that persons prosecuted for espionage under national law are entitled to due process under international human rights law, the recent emergence of cyber espionage utilizing extraordinarily effective computer viruses such as Flame and Gauss may require a rethinking of the conventional wisdom. Admittedly, reaching agreement on the rules of international law that would govern cyber espionage might be an impossible mission.

---

136. *See* John F. Murphy, *Mission Impossible? International Law and the Changing Character of War*, 41 ISRAEL YEARBOOK ON HUMAN RIGHTS 1, 4 (2011).

When all is said and done, it is highly likely that the legal issues surrounding cyber war and related cyber activities are not the most important challenge facing the United States and its allies. If Richard Clarke is right that although the United States has developed a so far unmatched capacity to conduct an offensive cyber war, it has virtually no *defense* against the cyber attacks he says are targeting us now, and will be in the future;[137] the greater urgency is to remedy this situation. A major obstacle to resolving this problem is the resistance of private industry to governmental efforts to induce businesses to improve their cyber security. It is clear, however, that government and private business cooperation will be indispensable if U.S. defenses against cyber attack are going to be effective.

137. *See supra* note 71 and associated text.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Organizing for Cyberspace Operations: Selected Issues

Paul Walker

89 INT'L L. STUD. 341 (2013)

Volume 89 2013

Organizing for Cyberspace Operations: Selected Issues

Paul Walker[*]

I. INTRODUCTION

The United States dramatically raised the profile of cyberspace operations as a method of warfare when it announced the establishment of the United States Cyber Command in June, 2009.[1] As a sub-unified command of the United States Strategic Command and led by a four-star general, who also serves as the Director, National Security Agency, Cyber Command absorbed the responsibilities of two separate, lower-profile organizations: Joint Task Force-Global Network Operations (JTF-GNO) and Joint Functional Component Command-Network Warfare (JFCC-NW).[2]

* Commander, Judge Advocate General's Corps, U.S. Navy; Deputy Director, Office of the Judge Advocate General's Information Operations (Cyber) and Intelligence Law Division. The views expressed here are Commander Walker's personal opinion and do not necessarily represent the views of the Department of Defense, the Department of the Navy, the Naval War College or United States Cyber Command.

1. Memorandum from Secretary of Defense Robert M. Gates to Secretaries of the Military Departments et. al, Establishment of a Subordinate Unified U.S. Cyber Command Under U.S. Strategic Command for Military Cyberspace Operations 1 (June, 23, 2009), *available at* http://fcw.com/~/media/GIG/GCN/Documents/cyber%20command%20gates%20memo.ashx.

2. *Id.* at 1–2.

There were a number of reasons for creating Cyber Command. First, bringing together JTF-GNO and JFCC-NW eliminated deficiencies and gaps between those operating Department of Defense (DoD) networks and those charged with defending the same networks.[3] Second, the newly realized efficiencies would result in an increased ability to support global missions with cyberspace operations.[4] Finally, deficiencies and gaps in DoD's cybersecurity efforts were identified in response to specific intrusion events into DoD networks.[5] Operation Buckshot Yankee, the DoD response to "the most significant breach of U.S. military computers ever" in 2008, was a key impetus to the standup of Cyber Command, according to then-Deputy Secretary of Defense William Lynn.[6] Although Cyber Command will "integrate cyberdefense operations across the military"[7] through its mission to "direct the operations and defense of specified Department of Defense information networks,"[8] the command also has the responsibility for conducting offensive operations in cyberspace.[9]

In the ensuing three years, Cyber Command reached full operational capability on October 31, 2010.[10] As that occurred, countries around the world established or announced plans to create their own cyberspace commands. Some, such as China, India and Russia, apparently tied the creation of their units directly to the creation of Cyber Command.[11] Like the United States, other countries are establishing such a unit in response to

3. Conference Brief, Cyber War and International Law, Panel I: An Introduction to Cyber Operations 1 (remarks of Colonel Ron Reed, U.S. Air Force (Ret.)), http://www.usnwc.edu/getattachment/97cfcf32-5007-4b2c-b1a8-8fb7b8cd2e4f/ILD-Conference-Brief-2012.aspx (last visited Sept. 30, 2012).

4. *Id.* at 1–2 (remarks of Captain Timothy J. White, U.S. Navy).

5. *Id.* at 1.

6. William J. Lynn III, *Defending a New Domain*, FOREIGN AFFAIRS, Sept.–Oct. 2010, at 97.

7. *Id.*

8. Fact Sheet, United States Strategic Command, U.S. Cyber Command (Dec. 2011), http://www.stratcom.mil/factsheets/Cyber_Command/.

9. *See id.* The third mission assigned to Cyber Command is "when directed, conducts full-spectrum military cyberspace operations."

10. *Id.*

11. *See* Tania Branigan, *Chinese Army to Target Cyber War Threat,* GUARDIAN (London) (July 22, 2010, 2:31 PM), http://www.guardian.co.uk/world/2010/jul/22/chinese-army-cyber-war-department); Harish Gupta, *India Setting Up Cyber Command*, MSN NEWS (May 15, 2011, 6:51 PM), http://news.in.msn.com/national/article.aspx?cp-documentid=5160226#page=1; *Vice Prime Minister Rogozin Pledges to Set Up Cyber Command in Russia*, CNEWS, (Mar. 22, 2012, 3:15 PM), http://eng.cnews.ru/news/top/indexEn.shtml?2012/03/22/482544.

external threats. In the case of South Korea, the threat is cyber actions emanating from North Korea.[12] For Iran, the decision to create a cyber command came a year after the world learned about the Stuxnet virus, which caused damage to nearly one thousand centrifuges at an Iranian nuclear facility.[13] Still other States had cyberspace operations units that predated the creation of Cyber Command, but whose existence only became public in the years following Cyber Command's establishment. Germany and the United Kingdom are two such examples.[14]

These are just the most prominent examples of States that have taken or are preparing to take such a step. There are undoubtedly others who have created such units in greater secrecy or whose action went unnoticed by the Western media. As more and more States create computer network operations or cyber command units, it is appropriate to examine the international law implications for how such units should be organized to conduct operations given the unique nature of cyberspace as an operating domain.

This article examines three areas of the law of armed conflict with implications for the organization and execution of cyberspace operations. Of necessity, given the little information that is available from most States with respect to cyberspace operations and the prominence of the Cyber Command, these areas will be examined through the prism of DoD practices. Part II examines the issue of reviewing cyberspace weapons for compliance with the law of armed conflict, comparing and contrasting the practices of the services that comprise the U.S. armed forces. Part III addresses the issues that occur in organizing for cyberspace operations raised by the requirement to take precautions against the effects of attacks. Specifically, the section will examine the feasibility of clearly separating military objects and objectives from civilian objects in cyberspace. Part IV extends the discussion of precautions against the effect of cyber attacks to a State's conduct

12. *See* Jung Sung Ki, *Cyber Warfare Command to be Launched in January*, KOREA TIMES (Dec. 1, 2009), http://www.koreatimes.co.kr/www/news/nation/2009/12/205_56502.html (describing suspicions that North Korea was behind massive distributed denial of service attacks occurring against government and industrial sites earlier in the year).

13 *Iran to Launch First Cyber Command,* PRESSTV (Mar. 25, 2012, 6:02 PM), http://presstv.com/detail/184774.html.

14 John Leyden, *Germany Reveals Secret Techie Soldier Unit, New Cyberweapons*, THE REGISTER (June 8, 2012, 11:29 AM), http://www.theregister.co.uk/2012/06/08/germany_cyber_offensive_capability/; Colin Clark Monday, *Stratcom Plows Ahead on Cyber*, DOD BUZZ (June 29, 2009, 11:51 AM), http://www.dodbuzz.com/2009/06/29/stratcom-plows-ahead-on-cyber/.

of its own cyber attacks, examining principles implicit in the interaction between a number of customary rules within the law of armed conflict to arrive at an explicit conclusion as to how States should organize and prepare for conducting cyber attacks.

II. WEAPONS REVIEWS

Article 36 of Additional Protocol I obligates States that develop, acquire or adopt "a new weapon, means or method of warfare . . . to determine whether its employment would, in some or all circumstances, be prohibited" by the law of armed conflict.[15] The determination is to be made in the course of the acquisition or development of the weapon, means or method of warfare in order to ensure it can be employed within the law of armed conflict.[16] The rule recognizes the practicality of ensuring that a new weapon, means or method of warfare can be legally used before a State expends the often-considerable expense of procuring it.

Of course, it may not be apparent at that early stage whether the weapon will actually be employed as it was intended to be used during the course of its development. In addition, prohibitions on a weapon's use may be factually dependent and not all of those situations may be foreseeable during a legal review that occurs during the course of acquisition or development. Thus, in order to meet the requirement of examining the weapons legality "in some or all circumstances,"[17] it may be necessary to conduct more than one legal review of the weapon, not only during acquisition or development, but also prior to employment of the weapon by a State's operational forces.[18]

Neither Article 36 nor the *Commentary* on Additional Protocol I define what is meant by the term "weapon, means or method of warfare." In fact,

15. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 36, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

16. *Id.*

17. *Id.*

18. Harold Hongju Koh, Legal Adviser, U.S. Department of State, International Law in Cyberspace, Keynote Address at the USCYBERCOM Inter-Agency Legal Conference 4 (Sept. 18, 2012) (transcript on file with author). ("The U.S. Government undertakes at least two stages of legal review of the use of weapons in the context of armed conflict—first, an evaluation of new weapons to determine whether their use would be *per se* prohibited by the law of war; and second, specific operations employing weapons are always reviewed to ensure that each particular operation is also compliant with the law of war.").

the *Commentary* only uses the term "weapon" and does not address potential differences, if any, between a weapon and the ostensibly broader "means or method of warfare."[19] If one considers that the purposes of the law of armed conflict are to prevent unnecessary suffering to both combatants and noncombatants, as well as to prevent harm to civilians and civilian objects from attacks, weapons are the devices that are used in attacks to cause such suffering. Unlike "weapon," there is a definition of "attack" as an "act of violence, whether in offence or defense," contained in Article 49 of Additional Protocol I.[20] Given the uncertain application of the law of armed conflict in the cyber domain, recent scholarship has focused on the question of what the definition of "attack" means by way of resulting effects or consequences.[21] The emerging consensus is that for a military action, whether it occurs in cyberspace or not, to be considered an "attack," it must result in a violent consequence such as death, injury, or physical damage to property.[22] Weapons, then, are the devices used in attacks that cause the deaths, injuries or damage to property. As will be seen, this view is consistent with the definitions of "weapon" used by the armed forces of the United States.

U.S. practice is to conduct multiple legal reviews of weapons in order to meet the requirements of customary international law as reflected in Article 36. The first review is "an evaluation of new weapons to determine whether their use would be *per se* prohibited by the law of war."[23] In U.S. practice, this acquisition weapons review is generally conducted by the service—Army; Navy, including the Marine Corps; or Air Force—that is pro-

19. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶¶ 1463–1482 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987).

20. Additional Protocol I, *supra* note 15, art. 49.

21. *See, e.g.*, Michael N. Schmitt, *Cyber Operations and the* Jus in Bello*: Key Issues*, *in* INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 89, 94 (Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies) ("A cyber operation, like any other operation, is an attack when resulting in death or injury of individuals, whether civilians or combatants, or damage to or destruction of objects, whether military objectives or civilian objects."); Paul A. Walker, *Rethinking Computer Network "Attack": Implications for Law and U.S. Doctrine*, 1 NATIONAL SECURITY LAW BRIEF 33, 47 (2010).

22. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE rule 30 (Michael N. Schmitt ed., 2013), ("A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.") [hereinafter TALLINN MANUAL].

23. Koh, *supra* note 18, at 4.

curing the weapon. Once a determination is made to employ a weapon, the operation is reviewed to ensure that, in the specific factual context, the weapon's use complies with the law of armed conflict.[24] This second review is completed by the unit employing the weapon. For U.S. military cyberspace operations, that unit is currently Cyber Command.

The acquisition review requirement is formally established in Department of Defense Directive 5000.1, "The Defense Acquisition System," which vaguely states "[t]he acquisition and procurement of DoD weapons and weapon systems shall be consistent with all applicable domestic law and treaties and international agreements . . . customary international law, and the law of armed conflict."[25] With respect to cyber weapons, this requirement has been implemented differently by each of the Services. In 2011, the Air Force rewrote its instruction to require not only legal reviews of "weapons," but also legal reviews of "cyber capabilities," which are broadly defined to include almost any effect created in cyberspace, not just the types of effects (death and injury to persons and damage to property) caused by weapons.[26] The naval service (Navy and Marine Corps) also revised its acquisition instruction in 2011, but did not similarly single out cyber capabilities. Instead, the Navy guidance defines weapons that must undergo legal review as items "that are intended to have an effect of injuring, damaging, destroying, or disabling personnel or property, to include non-lethal weapons."[27] The Army's instruction is older, being last revised in 1979. It also focuses on items that have "an intended effect of injuring, destroying, or disabling enemy personnel, materiel, or property" as weapons.[28] Army practice has been to conduct acquisition legal reviews of cyber capabilities if one is requested, but not as a matter of course. Given that the Air

24. *Id.*

25. Deputy Secretary of Defense, DoD Directive 5000.01, The Defense Acquisition System encl. 1, ¶E1.1.15 (2003, current through Nov. 20, 2007), *available at http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf.*

26. Secretary, Department of the Air Force, AFI 51-402, Legal Reviews of Weapons and Cyber Capabilities (2011), *available at* http://www.fas.org/irp/doddir/usaf/afi51-402.pdf [hereinafter AFI 51-402].

27. Under Secretary of the Navy, SECNAVINST 5000.2E, Department of the Navy Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System ¶ 1.6.1.c (2012), *available at* http://www.acquisition.navy.mil/ content/download/7754/35836/.../5000+2e.pdf.

28. Headquarters, Department of the Army, Army Regulation 27-53, Review of Legality of Weapons Under International Law ¶ 3.a, Jan. 1, 1979, *available at* http://www.fas.org/irp/doddir/army /ar27-53.pdf.

Force instruction is the only one to single out cyber capabilities, it is instructive to examine that guidance in more detail.

First, it is important to understand that the Air Force instruction does define "weapons" in a manner similar to the other Services: "devices designed to kill, injure, disable or temporarily incapacitate people, or destroy, damage or temporarily incapacitate property or materiel."[29] It then goes on to separately define "cyber capability" as "any device or software payload intended to disrupt, deny, degrade, negate, impair or destroy adversarial computer systems, data, activities or capabilities."[30] The only exception to the breadth of this definition is a "device or software that is solely intended to provide access to an adversarial computer system for data exploitation."[31] Otherwise, the full review procedures provided in the instruction apply equally to both weapons and cyber capabilities, including any and all modifications to those weapons and cyber capabilities. Thus the Air Force instruction meets the requirements of Article 36 by basically requiring the same type of review for the same types of weapons as the other Services. The guidance to also review cyber capabilities is not required by Article 36, but is a policy choice made by the Air Force. Of course, nothing in the law of armed conflict prohibits States from doing more than the minimum required by those laws. In this case, however, the additional review requirements do very little to advance the purposes of the law of armed conflict and, in fact, result in misapplying its principles. In addition, by not limiting the legal review to those cyber capabilities that are intended to cause destruction of property, deaths or injuries, the over-inclusive definition unnecessarily impedes operations, particularly given the Air Force requirement to conduct a new legal review for any modification of a cyber capability.

As discussed earlier, weapons reviews are conducted to ensure they do not violate prohibitions against unnecessary suffering to combatants and noncombatants, as well as ensuring that the use of the weapon does not result in indiscriminate attacks on civilians or civilian objects, this latter purpose is embodied in the principle of distinction. The problem with the Air Force approach to having all cyber capabilities reviewed is that most of the capabilities acquired will not have the effect or intent of causing any human suffering, much less death or injury. Other than the possible destruction of adversary computer systems, the other types of capabilities that

29. AFI 51-402, *supra* note 26, attachment 1.

30. *Id.*

31. *Id.*

must be reviewed—those that disrupt, deny, degrade, negate or impair computer systems, data, activities or capabilities—in most cases, if not all, will have little to no destructive impact on property. Where there is no intent or ability for the cyber capability to produce the same effects as a weapon used during an attack, then the legal review becomes a needless exercise in paper production.

From an operational perspective, such unnecessary administrative requirements impede the ability to conduct operations in a timely manner, particularly in the area of cyberspace operations where exhortations to move at "net speed" predominate. As a policy matter, it is understandable to place an excess of caution into this developing area and, ideally, operational impacts of extra review requirements are limited when the reviews occur during the acquisition process prior to procurement and deployment to or by operational forces. Unfortunately, the Air Force instruction does not mitigate the operational impact, but, instead, exacerbates them by requiring that cyber capabilities that are modified must undergo a new legal review.[32] This new review must be performed within Air Force channels, even if the capability has been operationally deployed. The instruction also does not provide a *de minimus* exception that would permit minor alterations to go unreviewed, even if the alteration does not change the effects to be delivered by the capability in any way. This is a real problem for the conduct of operations. Unlike kinetic weapons, cyber capabilities are routinely modified during the course of employment to account for changes in the operational environment, new versions of operating systems, software updates, changes to anti-virus software, and installation or updating of system firewalls. These types of alterations or modifications, where there is no change to what the capability does, are best left to the operational legal review prior to employment, rather than reinserting them into the acquisition process.

For States organizing for cyberspace operations, an examination of U.S. practice demonstrates the best way to comply with the requirement to conduct legal reviews of new weapons. Cyber capabilities should only undergo a legal review as a "new weapon" when the cyber capability is developed with the expectation or intent that its use will result in death, injuries, or damage or destruction of property. This is consistent with current practice with respect to kinetic weapons and is the approach taken by the U.S. Army and the naval service. The law of armed conflict does not require legal

32. *Id.*, ¶ 1.3.

reviews of all new, and newly-modified, cyber capabilities, as is the current Air Force practice. Instead, cyber capabilities whose use is not expected or intended to result in death, injuries or damage to property should only be subjected to a legal review at the time they are employed as part of the legal review undertaken to ensure that the operation as a whole complies with the law of armed conflict.

III. PRECAUTIONS AGAINST THE EFFECTS OF ATTACKS

When preparing to conduct cyberspace operations, States need to be cognizant of the obligations that the law of armed conflict imposes with respect to protections for the State's own populace. Applying these obligations in cyberspace operations yields different outcomes than those that result from preparing for kinetic operations. Instead of focusing on physical separation of civilians and civilian objects, States that undertake cyberspace operations may need to focus on conducting these operations in such a way that civilian cyber objects are not mistaken by potential adversaries for the State's own cyber military objects and objectives.

The general obligation to take precautions against the effects of attacks occurring within a State's own territory is contained in Article 58 of Additional Protocol I and is written in distinctly "kinetic" terms. It is a three-part obligation that involves "remov[ing] . . . civilians and civilian objects . . . from the vicinity of military objectives";[33] not "locating military objectives within or near densely populated areas";[34] and taking "other necessary precautions to protect . . . civilians and civilian objects . . . against the dangers resulting from military operations."[35] Of these three, the easiest one to apply directly to cyberspace operations on its own terms is the third one, to take necessary precautions to protect against the dangers resulting from military operations. In the kinetic sense, the commentary on this article makes clear that, when drafted, this portion of the article referred to a State's provision of civil defense measures for its population, such as bomb shelters.[36] The commentary also discusses a State's provision of civil defense services and the training and equipping of civil defense forces. In the context of cyberspace operations, cybersecurity measures undertaken by a State to protect civilian cyber infrastructure are equivalent to the types of

33. Additional Protocol I, *supra* note 15, art. 58(a).
34. *Id.* art. 58(b).
35. *Id.* art. 58(c).
36. *See* COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 19, ¶¶ 2239–57.

civil defense measures contemplated by sub-paragraph (c) of Article 58. Of course, unlike State-sponsored and State-provided civil defense measures, there are a multiplicity of means and mechanisms available for undertaking cybersecurity measures. What Article 58(c) makes clear, though, is that at least to some extent the obligation is a State responsibility and is not something that can be left solely to the private sector to implement. How such measures are to be implemented by States is left to their discretion, but Article 58 makes clear the State's obligation to do something.

The other two provisions of Article 58 concern physical separation between military and civilian objects. This obligation to clearly separate and distinguish between civilian objects not subject to attack by an adversary and military objects that are properly subject to attack serves to aid in the adversary's ability to adhere to the law of armed conflict principle of distinction. The obligations contained within Article 58 are not absolute, however. Instead, they must be undertaken "to the maximum extent feasible," which is described in the *Commentary* as not being required "to do the impossible." [37] Over time, a consensus has emerged that the feasibility requirement means that States must do what is practicable and are not required to take steps that are impracticable. The practicality approach is taken by the numerous compilations of customary international law applicable to specific warfighting domains, such as the *Air and Missile Warfare Manual*,[38] the *San Remo Manual*[39] and with respect to cyberspace operations, the *Tallinn Manual*.[40]

On the flip side of the obligation to segregate military from civilian objects is a requirement not to intentionally intermingle such objects, particularly if the goal is to use an object's civilian or other protected status as a means of protecting the military object from attack. On this aspect of precautions against the effects of attacks, the *Air and Missile Warfare Manual*'s discussion of customary international law is explicit: "Belligerent parties subject to air or missile attacks must, to the maximum extent feasible, avoid locating military objectives within or near densely populated areas, hospi-

37. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 19, ¶ 2245.

38. PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, COMMENTARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE rule 42 (2010), *available at* http://ihlresearch.org/amw/Commentary%20on%20the%20HPCR%20Manual.pdf.

39. SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA ¶ 46.3 (Louise Doswald Beck ed., 1995).

40. TALLINN MANUAL, *supra* note 22, at 147.

tals, cultural property, places of worship, prisoner of war camps, and other facilities which are entitled to specific protection. . . ."[41] Examples of State action violating this obligation occurred during the Gulf War to oust Saddam Hussein's forces from Kuwait. The Iraqi Air Force repeatedly removed combat aircraft from airfields and located them next to mosques within populated areas. Despite this intentional attempt to shield them from bombing, the aircraft remained valid military targets subject to attack, with any damage that might occur to the mosque required to be accounted for within the proportionality analysis by the attacking State. Although this example involves the intentional relocation of a military object next to a civilian protected object, the law of armed conflict also prohibits States from misusing the protected status of civilian objects during the course of attacks.

The question then becomes, what measures are practicable for States to take in separating their military cyber objects from civilian cyber objects. At first blush, it may not seem practicable at all given the ubiquitous nature of cyberspace. After all, the Internet grew out of a project started by the Defense Advanced Research Projects Agency, with an original intent of providing for redundant communication paths. From quite modest beginnings has grown a global phenomenon, with most of the supporting infrastructure in the hands of commercial entities. Cyberspace, the overarching term for not just what is known as the Internet, but the interaction of all connected networks and systems is heavily used by governments; industry, including government contractors; businesses, large and small; and by individual citizens of every country. Often, military communications (usually heavily encrypted) are traveling with and alongside all these other communications, particularly across the backbone infrastructures owned by what are known in the United States as "Tier 1 Internet Service Providers" and their equivalents in other countries.

At least one commentator who has written extensively in this area has declared that in the context of cyberspace operations "segregation of military and civilian objects during an armed attack [is] unfeasible."[42] Having concluded that it is not possible for States to meet the obligations of Arti-

41. PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE rule 42 (2009) [hereinafter AMW MANUAL].

42. Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks*, 88 TEXAS LAW REVIEW 1533, 1535 (2010).

cle 58(a) and (b),[43] his analysis focuses on the Article 58(c) obligations imposed on States to take cybersecurity measures to secure their civilian populations and companies from the effects of cyber attacks.[44] In a similar fashion, the newly-published *Tallinn Manual*'s Rule 59 on "Precautions against the Effects of Cyber Attacks" focuses on Article 58(c)'s requirement to take precautions to protect civilians and civilian objects from dangers arising from cyber attacks, and does not specifically address the physical differentiation addressed in Article 58(a) and (b).[45] The commentary on the *Manual*'s Rule 59 makes clear that the Group of Experts that authored the *Manual* viewed the obligations of Article 58(a) and (b) as subsumed within the rule they crafted.[46] In their view, sections (a) and (b) of Additional Protocol I's Article 58 are redundant with section (c). The commentary does mention actions such as "segregating military from civilian cyber infrastructure,"[47] but its only substantive discussion of the concept is to make the point that "[i]t may not always be feasible for parties to the conflict to segregate potential military objectives from civilian objects."[48] The focus of the *Tallinn Manual*'s commentary on Rule 59 is very much on what it characterizes as "passive precautions,"[49] rather than the arguably more active requirements of the other two sections of Article 58. Omitting a separate rule emphasizing and discussing the need for States to ensure physical separation of military from civilian cyber infrastructure unfortunately deemphasizes that aspect of the customary international law requirement to take precautions to protect their civilian populations from the effects of cyber attacks. Rather than downplaying this requirement, where the risk to civilian objects is as prevalent as many assume it is during cyberspace operations, the better course would have been to provide a number of more specific rules addressing these requirements in the specific cyber context. This was the approach taken by the *Air and Missile Warfare Manual*, which derived multiple rules addressing physical separation of military targets from civilians and civilian objects.

It is important, though, to differentiate between military cyber objects and dual-use objects, such as power plants or air traffic control systems,

43. *See id.* at 1542–52.
44. *See id.* at 1552–55.
45. TALLINN MANUAL, *supra* note 22, at 146.
46. *Id.*
47. *Id.*
48. *Id.* at 147.
49. *Id.*

that may be valid military objectives for attack by virtue of the fact that their nature, location, purpose and use makes an effective contribution to military capability. In many respects, dual-use objects, by their very nature and definition, are not subject to segregating their military value from their civilian nature or often from their civilian surroundings. But while Article 58's obligations are directed at both dual-use and sole-use military objectives, the above discussion makes clear that there is too much focus on dual-use objectives and not enough focus on those that are purely military in nature, whether fixed or mobile.

In cyberspace, State practice, particularly that of the United States, makes clear that it is feasible to separate purely military objectives from civilian objectives, at least up to a point. The United States military uses multiple, dedicated networks to conduct administrative, logistical and operational activities.[50] The three best-known networks are the Non-Classified Internet Protocol Router Network (NIPRnet, which carries information classified up to and including Sensitive but Unclassified), Secret Internet Protocol Router Network (SIPRnet, which carries data classified up to and including the Secret level) and the Joint Worldwide Intelligence Communication System (JWICS carries data classified up to and including Top Secret/Sensitive Compartmented Information). JWICS and SIPRnet are secure data transmission services, including voice over Internet Protocol services used for the transmission of classified information between DoD entities and between DoD and other parts of the U.S. government. Both networks are used for transmitting e-mail and web services, and for file transfer operations. SIPRnet is the main transmission method for operational command and control systems, such as the Global Command and Control System and the Defense Message Service used to communicate at the tactical and strategic levels between DoD commands.

The NIPRnet is an unclassified data service that uses the Internet Protocol for connecting to the public Internet. Like the two classified networks, the NIPRnet provides a transmission method for e-mail applications, web services and file transfers. The NIPRnet provides DoD commands and agencies with protected access to the Internet through a limited number of controlled Internet access points, or external network gateways. Protected, secure access between unclassified networks of DoD agencies, non-DoD agencies and departments, and the intelligence community oc-

50. The facts in the next two paragraphs are drawn from the website of the Defense Information Systems Agency, http://www.disa.mil (last visited Sept. 30, 2012).

curs through NIPRnet Federated Gateways. These two types of gateways serve to screen DoD's unclassified networks from the broader Internet and permit implementation of perimeter protection services for DoD networks, including the ability to filter web content and provide "secure DoD-wide Domain Name Service."[51] These activities serve to create "a clear boundary between DoD and others . . . and gives DoD some ability to maneuver at the boundary in response to cyber attacks."[52]

Although there are many military objectives (dual-use or otherwise) in cyberspace that are inextricably intermingled with civilian cyber objects, as has just been illustrated, there is a very substantial core of military cyberspace activity that occurs on and across dedicated military networks and systems. Here we have an intersection with the *Tallinn Manual*'s Rule 50, "Clearly Separated and Distinct Military Objectives," because these networks, most particularly the NIPRnet, present "clearly discrete cyber military objectives" even though they are connected to and integrated with cyber infrastructure used for civilian purposes. Thus, it is incorrect to characterize the Internet or even large portions of it as "dual-use" simply because it happens to carry military information alongside and with civilian information. In part, this is due to the fact that it is nearly impossible to determine the location and military significance of those communications at any given moment and concomitantly act against them. With respect to targeting U.S. infrastructure, characterizing the Internet as "dual-use" would be particularly problematic given the fact that the military networks discussed above are available for discrete targeting to achieve the same objectives.

For the organization of cyberspace operations, the object lesson is to ensure the use of dedicated military networks and systems for cyberspace operations that support the operations of a State's armed forces. Not only are such dedicated systems more easily defended, they also present the type of clearly separate and distinct military objective properly subject to attack. Dedicated military networks serve, therefore, to establish a virtual distinction akin to the physical separation or relocation that are the type of precautions against the effects of attack contemplated in the Article 58(a) and (b).

---

51. *Senstive but Unclassified IP Data*, DISA, http://www.disa.mil/Services/Network-Services/Data/SBU-IP (last visited Sept. 30, 2012).

52. *Id.*

IV. ORGANIZING TO CONDUCT CYBER ATTACK: MAKING THE IMPLICIT EXPLICIT

As States organize their forces to conduct cyber attacks, there is a need to make explicit that which is currently only implicit in the rules. Namely, that cyber attacks—those actions in cyberspace that are proximately intended to cause death, injuries or destruction of property—must not, to the maximum extent feasible, occur from, or be perceived as occurring from, civilian cyberspace objects such that a State responding to such cyber attacks would be induced to improperly direct its response against civilian cyber objects, whether in the attacking State or another State, rather than legitimate military objects and objectives. In other words, States must take care not to misattribute their cyber attacks to otherwise innocent civilian cyber objects and must segregate as much as they can the modes of conducting cyber attacks from civilian infrastructures. The purpose is to organize in such a way as to essentially take precautions against the effects of cyber attacks on a State's own civilian objects and objectives by ensuring they are not jeopardized by the manner in which that State conducts its own cyber attacks. The remainder of this section will discuss the rules from which this formulation is drawn, discuss the practicality of achieving such a solution given the previously discussed attributes of cyberspace and also discuss the operational practicalities that may result from conducting cyber attacks in this manner.

Article 57 of Additional Protocol I addresses the precautions to be taken by States during the planning and conduct of attacks. Other than the first paragraph, however, Article 57 discusses the measures an attacking State must take—the principles of distinction and proportionality—with respect to the objects of those attacks, with the presumption that such attacks are occurring in the territory of another State. Article 57(1) provides a more generic statement applicable to precautions in attack: "In the conduct of military operations constant care shall be taken to spare the civilian population, civilians and civilian objects." The commentary on Article 57 notes that this paragraph states a "general principle which imposes an important duty on belligerents with respect to civilian populations"[53] without distinguishing where those civilian populations are located. Here, the implication is that the general principle is applicable whether the civilian population is

53. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 19, ¶ 2191.

located in the State to be attacked, the attacking State or in a third State, without regard to whether that State is also a party to the conflict.

The previous section provided an extensive discussion of precautions against the effects of attacks required by Article 58. For purposes of this discussion, it should be noted that the requirements of that article refer to the precautions to be taken by a State with respect to its own population in order to mitigate the effects of attacks from another State. Although the text of the article does not directly address the issue presented in this section, it is implied in the article's application to situations involving certain types of military objectives, specifically weapons systems. One of the rationales for requiring, to the extent feasible, that weapons systems not be based or located within populated areas is that those particular military objects will be given a higher priority in targeting by the enemy precisely because they are the source of a State's own attacks against that enemy.

There are a number of customary international law rules that prohibit using specially protected places for purposes, such as the initiation of attacks, that would expose those places or objects to destruction or damage. For instance, there are well-developed rules against using cultural property and places of worship "in support of the military effort."[54] A similar customary international law rule is recognized with respect to medical units and personnel (including medical aircraft, ambulances and hospitals), though it is usually phrased in terms of whether those units are used to "commit, outside their humanitarian function, acts harmful to the enemy."[55] As these examples show, the law of armed conflict has long recognized, or at least felt the need to highlight, the need for specifically stated prohibitions on the use of certain protected places and personnel in the conduct of military operations in a manner that may expose those protected places and personnel to dangers from attack.

The lack of a similar specific prohibition on the use of all dedicated (not dual-use) civilian objects during the course of military operations may seem, at first glance, a surprising oversight. It may well be, though, that to the drafters of law of armed conflict treaties, particularly Additional Protocol I; there was no need to codify what was likely the most basic matter of common sense. After all, Additional Protocol I is replete with formulations of customary international law whose base presumption is the duty of State parties to protect civilians and civilian objects from the dangers of armed

54. Additional Protocol I, *supra* note 15, art. 53(b).

55. AMW MANUAL, *supra* note 41, rule 74.

conflict. The commentary on Article 58 even goes so far as to state an expectation that States "must also cooperate by taking all possible precautions for the benefit of their own population as is in any case in their own interest."[56]

Unfortunately, international law has not reached the point at which common sense reigns supreme with regard to cyberspace operations. Although the United States recognizes the applicability of the law of armed conflict to cyberspace operations and there is an emerging consensus among academics on this point as demonstrated by the recent publication of the *Tallinn Manual*, not all States share this view and still other States view the law of armed conflict's application as limited in nature, requiring new treaty law dedicated to these types of operations. These topics are an ongoing subject of discussions between the United States, China, Russia and other nations within the Group of Governmental Experts meeting under the auspices of the United Nations. Further complicating these matters, while there is a great deal of cyber activity ongoing, with much of it attributed to State actors, there has only been one even arguable instance of a cyber attack—the Stuxnet virus that operated against Iranian nuclear centrifuges. Probably, in part, because the Iranians never formally reported the results of Stuxnet as a use of force or an armed attack, the authors of the *Tallinn Manual* have even gone so far as to state that "[n]o international cyber incidents have, as of 2012, been unambiguously characterised by the international community as reaching the threshold of an armed attack."[57]

The custom and practice of States to this point in the cyberspace revolution has been much more focused on conducting espionage and exploitation activities in cyberspace, rather than its use as a means to conduct attacks. Although there is much public speculation about which States are behind specific activities, fueled by an increasing forensic competition between antivirus vendors such as Kaspersky, Symantec and McAfee, these activities are occurring in a manner such that they are not attributable to the sponsoring State. In his keynote address at the Naval War College's 2012 "Cyber War and International Law" conference, Professor Goldsmith addressed the characteristics of the cyber problem "that upend the traditional system," including the "difficulty of attribution."[58] Similarly, in his September, 2012, remarks at the Cyber Command legal conference, Harold

56. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 19, ¶ 2240.

57. TALLINN MANUAL, *supra* note 22, cmt. to rule 13, ¶13.

58. Conference Brief, *supra* note 3, at 4 (Keynote Address, Jack Goldsmith, Professor, Harvard Law School, National Security Law and Cyberspace).

Koh, Legal Adviser for the U.S. Department of State, discussed the challenges presented by the dual-use nature of the cyberspace environment and the difficult technical, policy and legal questions presented by attribution in cyberspace.[59] At the same time, Koh also downplayed their uniqueness to the cyber domain, stating that "[t]hese questions about effects, dual-use and attribution are difficult legal and policy questions that existed long before the development of cyber tools."[60]

Although the non-attributable manner of conducting espionage and exploitation activities in cyberspace is instructive as to how States may carry out cyber attacks in the future, it is not necessarily illustrative and should not be viewed as dispositive at this point in time. It is one thing to carry out espionage and exploitation activities in a manner that intermingles and hides among the civilian infrastructure of cyberspace and the Internet. That is, after all, exactly how espionage is conducted between nations in the physical world, though generally the spies are physically present on the territory of the other nation. The ten-member Russian spy ring discovered operating in various U.S. East Coast locations in 2010 is but the most recent example.[61]

It is quite another thing for States to routinely conduct military operations that cause death, injury or destruction of property during the course of an armed conflict in a manner that is not attributed to the State actor as a matter of course. Setting purely domestic considerations aside, as cyberspace operations move closer and closer to a demonstrated capacity to cause the same type of deaths, injury to persons and destruction of property as kinetic weapons, there will be substantial pressure on military forces to move away from the methodologies of espionage and exploitation in carrying out these cyber attacks. This pressure will occur not only because of the need to comply with customary international law as embodied in the articles of Additional Protocol I discussed earlier, but also because of the need for States to accept responsibility for their actions and the actions of their armed forces during the course of armed conflict. Again, without any available examples of cyber attacks, there is no ability to examine actual State practice in this area. This does mean, however, that there remains room and opportunity for States to conform their future cyberspace operations to the need to keep the military sources of their cyber attacks segre-

59. Koh, *supra* note 18, at 6.

60. *Id.*

61. *See, e.g.*, Scott Shane & Charlie Savage, *In Ordinary Lives, U.S. Sees the Work of Russian Agents*, NEW YORK TIMES, June 28, 2010, at A1.

gated from civilian cyber infrastructure, always, of course, to the maximum extent feasible.

As with the earlier discussion about precautions against the effects of cyber attacks, the question then arises whether it is feasible to conduct cyber attacks from a military cyber infrastructure that is segregated from civilian cyber infrastructure and possibly attributable as such. Given the existence of the dedicated NIPRnet that is virtually segregated from other portions of the civilian Internet infrastructure, the question as to feasibility of using separate military networks to conduct cyber attacks is an unqualified "yes." Another solution, relying on a component portion of the NIPRnet, was proposed some years ago in an *Armed Forces Journal* article.[62]

In that article, Colonel Williamson advocated using the af.mil network (the Air Force portion of the NIPRnet) to create a powerful robot network of computers (botnet) that could be used to "direct such massive amounts of traffic to target computers that they can no longer communicate and become no more useful to our adversaries than hunks of metal and plastic."[63] In Williamson's conception, this ability to "carpet bomb in cyberspace" would function as the cyberspace deterrent that the United States lacks. Building this botnet could occur by using the Air Force's existing servers and computers housing the service's intrusion detection systems or the botnet could be created by re-purposing the thousands of computers removed from service every year as part of the Air Force's annual technology refresh program. Those re-purposed computers could then be networked together using botnet software and made to deliver offensive effects for theater commanders. As the system matures, Williamson envisioned adding .mil machines from other portions of the NIPRnet and possibly computers from other U.S. government agencies.

Although such a system (and others like it) is certainly feasible, it may not be operationally practicable. For instance, the same Internet access points and federated gateways that provide the ability to provide protection at the interface with the civilian Internet would act as potential chokepoints that are easily mapped. Once known, the access points, as well as the system of botnets, may be easily defended against by blocking and filtering by an adversary. Williamson acknowledges the technical and engineering chal-

62. Charles W. Williamson III, *Carpet Bombing in Cyberspace: Why America Needs a Military Botnet*, ARMED FORCES JOURNAL, May, 2008, at 20, *available at* http://www.armedforcesjournal.com/2008/05/3375884.

63. *Id.* The remainder of this paragraph is drawn from this article.

lenges, but understands that those problems can generally be overcome by technical solutions.[64]

The issue of operational impracticability raises an interesting issue with respect to whether or not a technical solution remains feasible. In such a situation, a State would be in the position of declaring that something technically feasible is not practicable (and thus not really feasible under the law of armed conflict) because the State has a preferred way of conducting its operations. Though the law of armed conflict provides no ready answer to this dilemma, one of the key considerations is likely to be how much effort the State undertook to overcome the technical problems causing the operational impracticability. In addition, to the extent that the State chooses not to explore the feasibility of conducting cyber attacks from a segregated military cyber infrastructure, but instead conducts its military operations in a manner that intentionally intermingles those operations with civilian cyber infrastructure, problems would arise under the law of armed conflict.

V. CONCLUSION

As States organize for military operations in cyberspace, particularly the conducting of cyber attacks during the course of armed conflicts, they must remain fully cognizant of the burdens imposed by the law of armed conflict. Properly interpreted and applied, the law of armed conflict supplies the answers to many questions that will arise during the course of preparing to conduct cyberspace operations. The *Tallinn Manual on the International Law Applicable to Cyber Warfare* is an important contribution to the effort of addressing these questions. More importantly, the *Manual* provides a set of answers that is consistent in its viewpoint and approach, one that takes a cautious, yet prudent approach largely by analogy, in an area where very little State practice exists or is apparent.

As States conduct the legal reviews of cyber weapons required by the law of armed conflict, the example of U.S. practice is instructive. States should not follow the lead of the U.S. Air Force by requiring legal reviews of all cyber capabilities, but only those cyber capabilities whose intended effect or result is death, injury or destruction of property, the standard followed by the Army and the naval services.

64. *Id.*

When examining the precautions to be taken against the effects of cyber attacks, it is feasible to create—and easier to defend—dedicated military networks in an effort to establish separation, even if it is only virtual in nature, from a State's civilian cyber infrastructure. Likewise, cyberspace operations present unique challenges that, if not prepared for appropriately, will serve to further increase the risks to a country's innocent civilian cyber infrastructure if it executes cyber attacks from infrastructure that is intermingled with, and not segregated from, civilian cyber infrastructure. It is technically feasible to conduct cyber attacks in a manner that does not place civilian cyber infrastructure in increased jeopardy of attack. This area of the law of armed conflict is sure to come under additional scrutiny as States move closer to executing cyber attacks for which they accept responsibility during armed conflicts.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

The Road Ahead: Gaps, Leaks and Drips

Michael J. Glennon

89 INT'L L. STUD. 362 (2013)

Volume 89 2013

The Road Ahead: Gaps, Leaks and Drips

Michael J. Glennon[*]

I. INTRODUCTION

Might there be gaps in the international rules governing cyber conflict, and if so, are they likely to be filled? Is this the right way to think about these questions?

Whether gaps exist in international law seems at first to be a technical, almost marginal issue. On analysis, however, the question[1] emerges as one

---

* Professor of International Law, Fletcher School of Law and Diplomacy, Tufts University. This paper draws upon *The Dark Future of Cyber-Security Regulation*, 6 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 563 (2012). I thank Beau Barnes for research assistance and Cecile Aptel, William Banks, Robert Barnidge, Toni Chayes, Matt Hoisington, Peter Margulies, Michael Matheson, Vijay Padmanabhan, Alexandra Perina, Robert Sloane, Gary Solis and Cecilia Vogel for comments on an earlier draft. Errors and views are my own.

1. The literature on the broader question of lacunae and *non liquets* in international law is neither new nor thin. *See* MALCOLM N. SHAW, INTERNATIONAL LAW 92–93 (5th ed. 2003); Daniel Bodansky, Non Liquet *and the Incompleteness of International Law*, *in* INTERNATIONAL LAW, THE INTERNATIONAL COURT OF JUSTICE AND NUCLEAR WEAPONS 153 (Laurence Boisson de Chazournes & Philippe Sands eds., 1999); Ole Spiermann, Lotus *and the Double Structure of International Legal Argument*, *in id.* at 131; Prosper Weil, *"The Court Cannot Conclude Definitively . . .":* Non Liquet *Revisited*, 36 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 109 (1997); Julius Stone, Non Liquet *and the Function of Law in the International*

that goes to the very "source of validity of international law," rather in the manner that questions posed by quantum mechanics go to the heart of the physical structure of the universe.[2] Nowhere are the issues more urgent or far-reaching than in the realm of cyber war.

Press reports about Stuxnet[3] and related activities suggest the unease with which cyber activities fit within the framework of existing rules. Was "Olympic Games," the covert operation in which Stuxnet was employed, a use of force within Article 2(4) of the United Nations Charter? Did Olympic Games constitute an "armed attack" under Article 51—which would have permitted defensive use of force by Iran against the United States and Israel? Is this an international armed conflict governed by international humanitarian law? Is the United States unlawfully using civilians in combat—or are the persons at the keyboards combatants because they are directly participating in hostilities? If so, who are the combatants? The Central Intelligence Agency's computer staff? The officer who pushed the "enter" button? Does it matter whether they fail to "carry arms openly" or wear a "fixed distinctive sign recognizable at a distance"?[4] Can they be prosecuted if they're captured by Iran, or extradited to Iran by a friendly State?[5]

Community, 35 BRITISH YEARBOOK OF INTERNATIONAL LAW 124 (1959); Hersch Lauterpacht, *Some Observations on the Prohibition of "*Non Liquet" *and the Completeness of the Law*, *in* SYMBOLAE VERZIJL 196 (Marinus Mijhoff ed., 1958), *reprinted in* 2 HERSCH LAUTERPACHT, INTERNATIONAL LAW: COLLECTED PAPERS OF HERSCH LAUTERPACHT 213 (Elihu Lauterpacht ed., 1975); John Dickinson, *The Problem of the Unprovided Case,* UNIVERSITY OF PENNSYLVANIA LAW REVIEW 115 (1932).

2. *See* Stone, *supra* note 1, at 125.

3. *See, e.g.*, David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, NEW YORK TIMES, June 1, 2012, at A1.

4. *See* Convention Relative to the Treatment of Prisoners of War art. 2, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Prisoners of War Convention].

5. Similar questions arise in connection with drone strikes. *See* Gary Solis, *America's Unlawful Combatants*, WASHINGTON POST, Mar. 12, 2010, at A17. For thoughtful consideration of whether gaps exist in the rules governing detention during conflicts with non-State groups, see John B. Bellinger III & Vijay M. Padmanabhan, *Detention Operations in Contemporary Conflicts: Four Challenges for the Geneva Conventions and Other Existing Law,* 105 AMERICAN JOURNAL OF INTERNATIONAL LAW 201 (2011).

II. THE ILLUSION OF COMPLETENESS

Some of the articles in this volume and much general commentary[6] suggest that the *jus ad bellum* and *jus in bello* rules that might address such questions contain no gaps. The assumption appears to be that the rules are comprehensive, comprising categories like squares on a huge juridical quilt that covers every possible fact situation and leaves no legal question unanswered. The implication is that only one correct answer exists for every such question,[7] since a complete system would leave no room for multiple, equally correct, conflicting answers to the same question. Finding the correct answer is merely a matter of accurate classification: identify the characteristics of the activity in question, and then place it neatly within the appropriate legal category. That there exist gray areas on the margins of each category makes classification more difficult but does not defeat it. The right answer is out there, waiting to be discovered, embedded in "community values,"[8] earlier rules,[9] their overarching purposes or some other juridically endogenous source that transcends humanity's fleeting differences. Good lawyers everywhere ultimately will come to the same correct conclusion as to how ambiguities should be resolved and which category is the right one. The analytic process is thus a logical sequence of binary choices: something like Stuxnet is either a use of force or not a use of force, an attack or not an attack, armed or not armed, perpetrated by combatants or noncombatants, and so on. Categories like these have a clear core; if judges can identify that core, the rest of us can as well. Find it, make the right choice at each step,

---

6. For representative recent writings, see TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., forthcoming 2013), draft *available at* http://issuu.com/nato_ccd_coe/docs/tallinn_manual_draft/1#share.

7. For an argument along these lines, see "Judge Hercules'" ability to identify the one right answer in RONALD DWORKIN, LAW'S EMPIRE 239 (1986) ("I must try to exhibit [the] complex structure of legal interpretation, and I shall use for that purpose an imaginary judge of superhuman intellectual power and patience who accepts law as integrity. Call him Hercules.").

8. Community-values adherents typically flesh out the concept with reliance upon notions such as security, human dignity, social progress, quality of life and self-determination. *Cf.* Dickinson, *supra* note 1, at 128 (referring to "the idea that all the materials which enter into the construction of a new legal rule for an unprovided case must themselves be law").

9. *See id.* at 118 ("The notion that legal rules are so connected rationally that one can be deduced from others leads to the conclusion that in the last analysis there is no such thing as an unprovided case. . . . [T]he law for new cases is to be found inside the law itself and not by resort to considerations and ideas drawn from outside the field of technical law.").

work through an idealized, neatly deduced decision tree and a single, accurate conclusion will appear.

This view has obvious attractions. It eliminates the specter of a "legal vacuum" from which, it is supposed, believers in the rule of law ought naturally to recoil. It promises a Holy Grail of universality, the glimmering possibility that good intentions and assiduous effort will yield unanimity. It eradicates analytic confusion by giving every legal problem a crystalline answer. It provides emotional succor to those who seek refuge from the bewildering tangle of conflicting wants, needs and emotions that spring from cultural, political and philosophical differences. It removes the perilous possibility that a non-existent gap in the law might be claimed by waterboarders and their ilk as a pretext for violation. It gives judges an airtight rationale for deciding every case without trenching upon legislative or sovereign prerogatives, as the case may be, since adjudication always entails interpreting existing rules rather than making new ones. It counters the growing problem of fragmentation in the international system. And it eliminates the frustrating need to come to consensus on new rules: if no gaps need be filled, no new rules need be devised. For lawyers puzzling over the rules that govern cyber war, cyber attacks, cyber defense and the like, this view of law is beguiling.

It has but one drawback—it doesn't deliver on its promises.

It's the wrong way to think about international law generally and the wrong way to think about the law of armed conflict in particular. The approach has been rejected by the International Court of Justice (ICJ)[10] and dismissed by legal scholars for over a hundred years as arid formalism, legal fundamentalism, noble dreams, mechanical jurisprudence, mythmaking and various other pejoratives[11]—for understandable reasons.

---

10. *See infra* notes 34–35.

11. In Germany, formalism was critiqued by Philip Heck and other proponents of a "jurisprudence of interests." *See* Philip Heck, *The Jurisprudence of Interests: An Outline*, *in* THE JURISPRUDENCE OF INTERESTS 31 (M. Magdalena Schoch ed. & trans., 1948). In France, François Gény argued that formal legal sources were inadequate to address all legal questions. *See* FRANÇOIS GÉNY, MÉTHODE D'INTERPRÉTATION ET SOURCES EN DROIT PRIVÉ POSITIF (La. State Law Inst. trans., 1963); Richard Groshut, *The Free Scientific Search of François Gény*, 17 AMERICAN JOURNAL OF JURISPRUDENCE 14 (1972). In the United States, legal realists pressed for greater attention to the consequences that categories produced, suggesting the propriety of "rule skepticism" and "fact skepticism" in the classification process. *See* JEROME FRANK, COURTS ON TRIAL: MYTH AND REALITY IN AMERICAN JUSTICE (1949); Hans Kelsen, *The Pure Theory of Law: Its Method and Fundamental Concepts*, 50

Think back to the earliest years, the years in which the law of armed conflict was young and rules were few. Did these pioneering, stand-alone rules leave no gaps? The few early rules were isolated patches; the "quilt" of international humanitarian law, such as it is, emerged only gradually, over many years.[12] In the initial years of the law's development, numerous matters that were later to be addressed by the rules remained uncovered.[13] At what point in the law's evolution did it become all-encompassing, leaving no question unanswered, like the rules of chess? At what point did human imagination freeze, losing all capacity to exploit ambiguities in the existing rules? When, precisely, did the law's development end? With the Hague Convention of 1899,[14] or 1907?[15] With the four 1949 Geneva Conventions?[16] With the additional protocols of 1979?[17] When did the system become complete? How would we know if it were complete?

At regular historical intervals, of course, general, prophylactic principles (such as the Martens clause, discussed later) did emerge, the ultimate import of which was undifferentiated humanitarianism. Unless one takes some form of moral intuition as transforming itself inexorably into legal

---

LAW QUARTERLY REVIEW 474 (1934); Roscoe Pound, *The Ideal Element in American Judicial Decision*, 45 HARVARD LAW REVIEW 136 (1931).

12. *See generally* JOHN FABIAN WITT, LINCOLN'S CODE: THE LAWS OF WAR IN AMERICAN HISTORY (2012); *see also* GARY B. SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 3–10 (2010).

13. *See* Dickinson, *supra* note 1, at 116 ("In the seventeenth and the early part of the eighteenth century, when many of the lines of our present legal processes were laid down, it is fair to say that the problem of the unprovided case was taken for granted and not clearly envisaged as a problem at all.").

14. Convention with Respect to the Laws and Customs of War on Land, July 29, 1899, 32 Stat. 1803.

15. Convention No. IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2227.

16. Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Prisoners of War Convention, *supra* note 4; Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

17 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609.

rules,[18] however, precepts that mandate unspecified altruism can hardly be considered sufficient to obviate the need for additional, more particularized squares on the legalist quilt, such as, for example, prohibitions against the use of dumdum bullets or noxious gases. These specific prohibitions and myriad others like them were considered necessary precisely because generalized exhortations to good conduct left room for reasonable disagreement as to what was expected. No evidence exists to suggest that the law has arrived—or ever will arrive—at some millennial zenith beyond which no further refinement need be contemplated. Evolving human wants, needs and emotions will continue to produce the ever-changing mishmash of clashing, culturally variant preferences from which international law flows.[19]

Nor, for that matter, is there any reason to believe that further legalization would necessarily be a good thing. Concerns about "law-free zones" take as the starting point that legal regulation is better than no legal regulation. But this is not always true; whether a "legal vacuum" is desirable depends upon the alternative and the law's effects. African captives on a nineteenth-century slave ship would not likely have hailed international law's prohibition against visitation of the vessel and release of its human cargo as filling a welcome gap in customary rules governing the slave trade.[20] It is not self-evident that a rule classifying Stuxnet as an armed attack ultimately would promote international peace or security. Compared with the alterna-

---

18. For a comment on Michael Walzer's effort to apply his notion of "practical morality" to war, see Michael J. Glennon, *Pre-empting Proliferation: International Law, Morality, and Nuclear Weapons*, 23 EUROPEAN JOURNAL OF INTERNATIONAL LAW ___ (forthcoming 2012). Though much of the formalism that pervades international humanitarian law can be attributed to surviving ghosts of a naturalist worldview, additional forces are at play, including the influence in Europe of a civil law tradition with purportedly comprehensive codes, and, in the United States, the continued emphasis on appellate cases in legal education, implying no need to examine exogenous, contextual sources to predict case outcomes. *See* Karl N. Llewellyn, *Some Realism About Realism—Responding to Dean Pound*, 44 HARVARD LAW REVIEW 1222 (1931). The oft-repeated claim that "we are all realists now" has yet to embrace all within international law's "invisible college."

19. Prosper Weil put it well:

> Regardless of the judicial and scholarly endeavors to affirm the completeness of international law, the truth of the matter is that international law is not complete. No legal order is, because there is not, cannot be, and should not be a rule at hand for every concrete or new situation. . . . More than municipal law, international law is by its very nature riddled with gaps.

Weil, *supra* note 1, at 118.

20. *See* The Antelope, 23 U.S. (10 Wheat.) 66 (1825). *See generally* Jean Allain, *Nineteenth Century Law of the Sea and the British Abolition of the Slave Trade,* 78 BRITISH YEARBOOK OF INTERNATIONAL LAW 342 (2007).

tive of airstrikes, Stuxnet probably was cheaper and more effective, risked no casualties, might have averted a major war, and—at least until its sponsorship was leaked—set no untoward precedent. Would that legal regulation could always do so well: less, in the legal realm, sometimes is more.

Consider closely the analogical process involved in classifying Stuxnet and other cyber weapons and it becomes apparent that categorization involves much more subjectivity than the formalists suggest. The circumstances that led to an old rule's creation can be similar in some respects to current circumstances but different in others; which elements take priority? There exists no objective standard by which to identify the characteristics of an act or thing that are salient for classification purposes, or how much weight one characteristic is to be given relative to another, or the level of generality or particularity with which they are to be stated, or whether instrumentalities or effects are dispositive.[21] One often can pull the accordion

---

21. NATO States have consistently argued, for example, that the UN Charter limits only harm caused by traditional instrumentalities—weapons—rather than cutoffs of foreign aid, trade boycotts, economic sanctions or other activities that might have the same consequences as an armed attack. Matthew Waxman has concisely summarized the traditional understanding:

> The dominant view in the United States and among its major allies has long been that the Article 2(4) prohibition of force and the complementary Article 51 right of self-defense apply to military attacks or armed violence. The plain meaning of the text supports this view, as do other structural aspects of the U.N. Charter. For example, the Charter's preamble sets out the goal that "armed force . . . not be used save in the common interest." Similarly, Articles 41 and 42 authorize, respectively, the Security Council to take actions not involving armed force and, should those measures be inadequate, to escalate to armed force. Moreover, Article 51 speaks of self-defense against "armed" attacks. There are textual counter-arguments, such as that Article 51's more specific limit to "armed attacks" suggests that drafters envisioned prohibited "force" as a broader category not limited to particular methods. However, the discussions of means throughout the Charter and the document's negotiating history strongly suggest the drafters' intention to regulate armed force differently and more strictly than other coercive instruments. This interpretation has generally prevailed over alternatives. . . .

Matthew Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4),* 36 YALE JOURNAL OF INTERNATIONAL LAW 421, 427–28 (2011) (footnotes omitted). *See also* Duncan B. Hollis, *Why States Need an International Law for Information Operations*, 11 LEWIS & CLARK LAW REVIEW 1023, 1040–42 (2007). The State Department Legal Adviser, however, has indicated that "if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would, that cyber attack should equally be considered a use of force." Harold Hongju Koh, Remarks at the U.S. Cyber Command Inter-Agency Legal Conference: International Law in Cyberspace (Sept. 18, 2012), http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/. Why actual physical damage should be required to bring an activity within the scope of Article 2(4) of the Charter is not clear; an ineffectual, attempted attack em-

of analogy wide or push it tightly together without risk of being proven wrong.[22] Much the same can be said of efforts to establish the law's completeness and continuousness through reliance upon supposed community values and underlying purposes. The assertion that community values concerning use of force are "shared" is belied by extensive international opinion polling,[23] as well as State practice and *opinio juris*.[24] To the extent that consensus does exist, it must be formulated at so high a level of generality and embrace so many different values, policies and political preferences as to support multiple, equally compelling and sometimes conflicting conclusions. These can be overcome only by presupposing an international consensus that does not now exist and never did exist.[25] Thus formalist analysis easily becomes outcome oriented, producing, in the words of Hersch Lauterpacht, a "deceptive clarity":

> [A]pparent indecision [by the International Court of Justice] . . . may—both as a matter of development of the law and as a guide to action—be preferable to a deceptive clarity which fails to give an indication of the inherent complexities of the issue.
>
> In so far as the decisions of the Court are an expression of existing international law—whether customary or conventional—they cannot but reflect the occasional obscurity or inconclusiveness of a defective legal system.[26]

---

ploying chemical or biological agents would seemingly constitute a use of force notwithstanding the absence of physical consequences. If the physical consequences of economic sanctions or trade boycotts cause physical damage, ought they too to be considered a use of force?

22. For discussion of the levels-of-generality problem in customary law, see MICHAEL J. GLENNON, LIMITS OF LAW, PREROGATIVES OF POWER: INTERVENTIONISM AFTER KOSOVO 50–52 (2001).

23. *See* Glennon, *supra* note 18.

24. *See generally* GLENNON, *supra* note 22.

25. Advance Questions for Lieutenant General Keith Alexander, USA, Nominee for Commander, United States Cyber Command: Before the S. Armed Services Comm., 111th Cong. 11 (Apr. 15, 2010), http://www.armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf ("There is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force."). *Compare* Koh, *supra* note 21.

26. HERSCH LAUTERPACHT, THE DEVELOPMENT OF INTERNATIONAL LAW BY THE INTERNATIONAL COURT 152 (1982).

False claims of clarity aimed at concealing the obscurity and inconclusiveness of legal rules that might or might not apply to hard cases generate only incoherence. What make hard cases hard is their incommensurability and our inability to devise objective criteria that render them commensurable.[27] In fact, as Hart wrote, "[s]uch cases are not merely 'hard cases'"; the problem is that "the law in such cases is fundamentally *incomplete*: it provides *no* answer to the questions at issue in such cases."[28]

Some insist that, because legal categories have a clear core, the international legal system is not "defective" at all and that ostensible gaps disappear. Even assuming that the category in question does have a clear core, however, it is ambiguity *at the margins* that produces gaps—gaps that disappear only if it's assumed that every ambiguity is in the end spurious and has a single, correct resolution, or that nothing but law goes into the making and interpretation of law, or that a relevant, pre-existing rule always twinkles like some far-off star exerting emanations from a penumbra that light up the one correct answer. Yet how, again, do we know this? Sometimes the galaxy seems empty; other times the galaxy seems to contain equally radiant stars. The formalists present no standard to assess which star is brighter, insisting only that one *must* be brighter and that reasonable people *must* come to the same, unfalsifiable outcome. But legal rules are not like stars. They don't emit luminosity that can be measured.[29] We have only the naked eye to judge their proximity. Rules are made up, created by human beings. Sometimes, but not always, they're given a specified priority as against other rules, as in the case of constitutional rules versus statutes. But even then, the nearest rules can be so remote in time, subject, or specificity as to generate honest doubt about their applicability.[30] Conflicts can arise

27. *See* John Finnis, *On Reason and Authority in* Law's Empire, 6 LAW AND PHILOSOPHY 357 (1987).

28. H.L.A. HART, THE CONCEPT OF LAW 252 (2d ed. 1997) (emphases in original).

29. For the suggestion that normativity exists in gradations, see Prosper Weil, *Towards Relative Normativity in International Law?*, 77 AMERICAN JOURNAL OF INTERNATIONAL LAW 413 (1983).

30. General, elastic norms are sometimes considered principles rather than rules. Rules are more specific, less malleable and cover less. Rules were described by Pound as "precepts attaching a definite detailed legal consequence to a definite, detailed state of facts." Roscoe Pound, *Hierarchy of Sources and Forms in Different Systems of Law*, 7 TULANE LAW REVIEW 475, 482 (1933). Principles, in contrast, are more general and constitute "authoritative starting points for legal reasoning, employed continually and legitimately where cases are not covered or are not fully or obviously covered by rules in the narrower sense." *Id.* at 483. Pound thus regarded principles as "hortatory." Roscoe Pound, *For the "Minority Report,"* 27 AMERICAN BAR ASSOCIATION JOURNAL 664, 677 (1941). Holmes, too, was

among rules of the same priority, efforts to reconcile the rules can fail, reasonable disagreement can arise as to which prevails, and a court can fairly resolve the controversy either way[31]—or can decline to resolve the controversy at all in the belief that its writ does not extend to rulemaking. The word that describes such a situation is *gap*.

Nor is it an answer to say that gaps don't exist because judges fill the gaps. Whether gaps exist and whether judges should fill them are different questions. Of course judges *can* sometimes fill the gaps; whether they *may* do so depends upon the authority given them by the specific legal system in which they sit.[32] When the law yields no answer, judges not infrequently find themselves asked, in effect, to decide on the basis of personal politics or philosophy[33]—as they declined to do in the *Nuclear Weapons* advisory opinion, where the ICJ (not for the first time)[34] acknowledged a gap of ex-

---

skeptical of their utility. When on the Supreme Court, he invited his fellow justices to name any legal principle on which they relied, suggesting that he could show them how it could be used to decide the case under consideration either way. *See* LOUIS MENAND, THE METAPHYSICAL CLUB: A STORY OF IDEAS IN AMERICA 340 (2004). Principles concerning the meaning of sovereignty, such as the sovereign equality of States, non-intervention and related concepts, do cover gaps and might presage future cyber rules, but they're not concrete enough to resolve categorization problems that flow from rules, and some principles have been ignored so often by so many States that their vitality is questionable. Non-intervention is an example. *See* Peter Ackerman & Michael J. Glennon, *Building Liberty: The Right Side of the Law,* AMERICAN INTEREST (Sept.–Oct. 2007), http://www.the-american-interest.com/article.cfm?piece=313; GLENNON, *supra* note 22.

31. *See generally* JOSEPH RAZ, BETWEEN AUTHORITY AND INTERPRETATION: ON THE THEORY OF LAW AND PRACTICAL REASON 11 (2009) ("[W]e cannot expect the law of any one country to have a uniform way of demarcating the boundary between what belongs to it and what lies outside of it, let alone expect to find that all legal systems demarcate the boundary in the same way.").

32. The Supreme Court appeared to identify the point at which indeterminacy pushes law interpreting into lawmaking in the seminal political question case of *Baker v. Carr*, 369 U.S. 186 (1962), where it found itself barred from deciding a question that involved "a lack of judicially discoverable and manageable standards for resolving it; or the impossibility of deciding without an initial policy determination of a kind clearly for nonjudicial discretion. . . ." *Id.* at 217. Such questions are non-justiciable, it seems, because a gap in the law precludes their resolution.

33. "In these cases it is clear," H.L.A. Hart wrote, "that the rule-making authority must exercise discretion, and there is no possibility of treating the question raised by the various cases as if there were one uniquely correct answer to be found, as distinct from an answer which is a reasonable compromise between many conflicting interests." HART, *supra* note 28, at 132.

34. See, for example, *Barcelona Traction, Light & Power Co., Ltd.* (Belg. v. Spain) (Second Phase), 1970 I.C.J. 3, 33–34 (Feb. 5), in which the ICJ found that "international law has

actly the sort here at issue.[35] Some legal systems are hospitable to judges' making up rules in such circumstances;[36] others are not.[37] Legal systems draw different lines between law interpreting and law creating. Some judges acknowledge the distinction; others do not.[38] In any event, in the first instance and sometimes in the last—before the judges intervene, and when judges won't intervene—lawyers must look to their own judgment to advise

---

not established its own rules" concerning "the rights of states with regard to the treatment of companies and shareholders"; *Haya de la Torre* (Colom. v. Peru), 1951 I.C.J. 71, 80 (June 13), in which the Court stated that the applicable law did not "give a complete answer" to the asylum question at issue; and *Military and Paramilitary Activities in and Against Nicaragua* (Nicar. v. U.S.), 1986 I.C.J. 14, 135 (June 27), in which the Court, addressing the question whether international law placed restrictions on a State's military arsenal, declared that "in international law there are no rules, other than such rules as may be accepted by the State concerned, by treaty or otherwise, whereby the level of armaments of a sovereign State can be limited."

35. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 105(2)(E) (July 8). The specific issue on which the Court was unable to reach a conclusion concerned whether the threat or use of nuclear weapons would be lawful or unlawful in an extreme circumstance of self-defense, in which the very survival of a State would be at stake. Judge Vereshchetin wrote separately that in an advisory proceeding that presents such a lacuna, the Court "ought merely to state this" and "cannot be blamed for indecisiveness or evasiveness where the law . . . is itself inconclusive." *Id.* at 280. Judge Higgins, on the other hand, wrote separately to emphasize that applicable norms "indubitably exist" and that "the judge's role is precisely to decide which of two or more competing norms is applicable in the particular circumstances." *Id.* at 592.

36. *See generally* Stone, *supra* note 1. In *Banco Nacional De Cuba v. Sabbatino*, 376 U.S. 398 (1964), the United States Supreme Court was urged to decide the case on the merits because, it was argued, "United States courts could make a significant contribution to the growth of international law, a contribution whose importance, it is said, would be magnified by the relative paucity of decisional law by international bodies." *Id.* at 434. The Court declined the invitation. "[G]iven the fluidity of present world conditions," it concluded, "the effectiveness of such a patchwork approach toward the formulation of an acceptable body of law concerning State responsibility for expropriations is, to say the least, highly conjectural." *Id.*

37. It is notable that the jurisdictional grant of the International Court of Justice directs it not to decide all disputes as are submitted to it, but "to decide *in accordance with international law* such disputes as are submitted to it" (Statute of the International Court of Justice art. 38(1), June 26, 1945, 59 Stat. 1055, 33 U.N.T.S. 993 (emphasis added)), suggesting that a gap in international law would require judicial abstention.

38. One ought to be skeptical, Hart urged, about "ritual language used by judges" who claim to be "the mere 'mouthpiece' of the law which [they] do not make or mold." HART, *supra* note 28, at 274. Prominent jurists such as Holmes, Cardozo and respected Law Lords have recognized that there are "cases left incompletely regulated by the law," cases in which judges have an "inescapable" lawmaking task, and that "many cases could be decided either way." *Id.*

clients, and lawmakers must look to their own judgment to decide whether existing rules are adequate.[39] The rejoinder that a single correct answer awaits them, if only they have the wits to find it, is a conclusion, not an argument—and it is moreover a conclusion that, again, defies falsification (for no counterexample can be hypothesized that could show that no such answer exists).

All this applies with particular force to international law. International law does not present a neat sequence of straightforward binary choices between "A" and "Not A." Junctures that the formalists regard as forks along the way in fact present a third choice: *neither* "A" *nor* "Not A." The third choice is "*No law*." At these junctures, the category in question doesn't seem quite right, but rejecting that category doesn't seem entirely right either. These are questions on which the law is either non-existent or unclear, but the result is the same: reasonable people can differ.

Contrary to the formalists' fears, however, acknowledging ambiguity doesn't open the door to a law-free zone, because international law applies a default rule in such circumstances. Its default rule is the famous freedom principle, from the *Lotus* case.[40] The principle has it that in the absence of a rule a State is deemed free to act, and that a burden of persuasion falls upon the State that alleges some limitation or restriction on another State's freedom of action. The formalists are, perversely, in this sense right that there are no gaps in the international legal order; what would otherwise be a gap is filled with the rule that a State is free to act unless some other State has shown that the acting State has consented to a restriction or limitation on its freedom of action. This possibility of a third option in resolving a dispute concerning the applicability of a category is more than a kind of

---

39. Keeping the rules alive by adding more fine print, judicially or legislatively, may seem at first blush like moving toward a more complete system with fewer ambiguities. In fact, more rules can lead to more gaps, not fewer, as when the law specifies new categories to which rules apply but says nothing about categories *not* specified, implying *expressio unius est exclusio alterius*.

40. The words of the Permanent Court of International Justice in *Lotus* are worth recalling:

> International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot therefore be presumed.

S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, ¶ 44 (Sept. 7).

juridical afterthought, invented for dealing with legal uncertainty. The third option, the freedom principle, is an affirmation of State sovereignty that encapsulates the foundational architecture of the international legal order.

The *Lotus*'*s* notion that the system is wholly consent based is, in the end, simplistic, in the sense that the international legal order is hardly devoid of coercion. The system does not rest upon pure, unfettered consent by all within it; policymakers within States often do things that they don't want to do and refrain from doing things that they do want to do. Other States, international organizations, non-governmental organizations and influential national elites all exercise various forms of power; all narrow States' ability to choose freely. The difference between the international legal system and domestic legal systems lies, rather, in the immediacy, source, extent and consequences of coercion, and the structure of incentives or disincentives that results. If the notion of consent that the international order pictures is taken as a form of constructive rather than actual consent, however, the freedom principle provides a useful shorthand that emphasizes basic structural differences.[41]

Whatever the conceptual difficulties with the notion of consent, it remains true that unless a restriction is established, a State remains free to act. Universalists dislike the notion that anything not prohibited is permitted, for holding out as it does the ever-present possibility that a State might defeat universality by declining to consent to a rule or by later withdrawing its consent. One effort in the realm of international humanitarian law to supplant the freedom principle with a form of natural law has been to use the Martens clause to overcome the hurdle of State non-consent. The clause in various iterations appears in a number of international humanitarian instruments. One of the most recent and prominent versions is set out in Article 1(2) of Additional Protocol I, which provides as follows: "In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from dictates of public conscience."[42] The argument is that the Martens clause, as customary international law, carves out an exception to the freedom principle by imposing limitations on States to which they have not consented.

---

41. *See* MICHAEL J. GLENNON, THE FOG OF LAW: PRAGMATISM, SECURITY, AND INTERNATIONAL LAW 17–18, 33, 64–65 (2010).

42. Additional Protocol I, *supra* note 17.

This argument is unconvincing. The clause is not a one-sentence cure-all that forever resolves all future legal ambiguities that might be created by technological innovation.[43] Assuming that the Martens clause does constitute customary international law[44]—which may not be the view of the United States[45]—it's doubtful whether States such as the United States have consented to that rule outside of specific treaties in which it exists,[46] and more doubtful still that the vague terms of the clause[47] necessarily have the

---

43. *See generally* David Friedman, *Does Technology Require New Law?*, 25 HARVARD JOURNAL OF LAW AND PUBLIC POLICY 71 (2001).

44. In its advisory opinion on the *Legality of the Threat or Use of Nuclear Weapons*, the ICJ said that the clause "had proved to be an effective means of addressing rapid evolution of military technology," 1996 I.C.J. 226, ¶ 78 (July 8), and that it represents customary international law. *Id.*, ¶ 84.

45. In 1987, the Deputy Legal Adviser of the U.S. State Department, Michael J. Matheson, identified those provisions of Additional Protocol I that the United States considers customary international law. Article 1(2) was not among them. *See* Michael J. Matheson, *The United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions*, 2 AMERICAN UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 419, 425 (1987). "No retreat from or disavowal of the Matheson announcement has been issued by any branch or department of the U.S. government." SOLIS, *supra* note 12, at 134 n.68. For an indication that the United States interprets the clause merely as recognition of the continued validity of customary rules that have not been modified by treaty, see BURRUS M. CARNAHAN, CUSTOMARY RULES OF INTERNATIONAL HUMANITARIAN LAW, REPORT ON THE PRACTICE OF THE UNITED STATES 6-2 (1997) (prepared for the International Committee of the Red Cross).

46. The United States has declined to ratify Additional Protocol I. Matheson, speaking in his official capacity, said as follows:

> First, the United States will consider itself legally bound by the rules contained in Protocol I only to the extent that they reflect customary international law, either now or as it may develop in the future. . . . Second, Protocol I now cannot serve in itself as the baseline for the establishment of common rules to govern the operations of military alliances in which United States forces participate. . . . Third, Protocol I cannot now be looked to by actual or potential adversaries of the United States or its allies as a definitive indication of the rules that United States forces will observe in the event of armed conflict and will expect its adversaries to observe. . . .

Matheson, *supra* note 45, at 420.

47. Guidance prepared by the U.S. Department of the Army for military lawyers indicated that the Martens clause "is difficult to apply in practice. Specific obligations resulting from the 'laws of humanity . . .' are extremely difficult to agree upon. . . . Such broad phrases in international law are in reality a reliance upon moral law and public opinion." U.S. DEPARTMENT OF THE ARMY, PAMPHLET NO. 27-161-2, 2 INTERNATIONAL LAW 15 (1962).

drastic effect of broadly negating the application of the freedom principle.[48] The United Kingdom argued as follows in *Nuclear Weapons*:

> While the Martens Clause makes clear that the absence of a specific treaty provision on the use of nuclear weapons is not, in itself, sufficient to establish that such weapons are capable of lawful use, the Clause does not, on its own, establish their illegality. The terms of the Martens Clause themselves make it necessary to point to a rule of customary international law which might outlaw the use of nuclear weapons. Since it is the existence of such a rule which is in question, reference to the Martens Clause adds little.[49]

The same would apply to cyber weapons: it's still necessary to point to an applicable rule, and a gap in the rules can exist. Nowhere in *Nuclear Weapons* does the ICJ suggest that the gap it identified is any less a gap because of the Martens clause. As the Court's opinion indicates, international law can *apply* to a given matter even though it contains a gap.[50]

None of this is to suggest that the international regime governing cyber operations is a blank slate. That the civilizing constraints of the law of war are not automatically eclipsed by technological innovation is the enduring reminder of the Martens clause. Clichéd but true, precepts of international law that have taken shape over centuries are the received wisdom of the

---

48. The Court had a chance to say that, if it had wanted to, in the *Nuclear Weapons* advisory opinion, *supra* note 35, and was in effect invited by the General Assembly to revisit the *Lotus* decision, but it declined to do so. Waldemar Solf suggested that the meaning of the principles of humanity and dictates of public conscience referred to in the clause "must be accepted in the practice of the states," suggesting that the clause—like any other treaty provision—has the effect of merely continuing in force pre-existing norms of customary international law that are not rendered inoperable by the treaty's application. *Remarks of Professor Waldemar Solf*, 2 AMERICAN UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 481, 483 (1987).

49. Letter Dated 16 June 1995 from the Legal Adviser to the Foreign and Commonwealth Office of the United Kingdom of Great Britain and Northern Ireland, Together with Written Comments of the United Kingdom 48, filed in Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion (June 16, 1995), *available at* http://www.icj-cij.org/docket/files/95/8802.pdf.

50. Broad inapplicability, however, might merely be thought of as a broader gap; both connote ineffectuality but in different degrees. The notion of a law that applies but has no effect was famously derided by Anatole France. "The law," he wrote, "in its majestic equality, forbids the rich as well as the poor to sleep under bridges, to beg in the streets, and to steal bread." ANATOLE FRANCE, THE RED LILY 95 (LE LYS ROUGE) (Winifred Stephens trans., 1927) (1894).

ages, to be ignored by the digitally distracted at their peril. That international law does not unequivocally proscribe unleashing a computer virus to destroy centrifuges by changing the rotational speed of their motors[51] does not mean that it is irretrievably vague about using malware to bring down a civilian airliner by freezing its computerized avionics.

Nor do I proffer any new answer to the dilemma of when law interpreting begins and lawmaking ends, about how the needs of the present ought to be reconciled with the commands of the past, about when the impulses of the living ought to defer to the designs of the dead. We are still, to paraphrase Martin Amis, dozens of Henkins away from answers to those questions. I do suggest that the old lawyers' saying—*Le mort saisit le vif,* the dead grip the living—has it backward: the living grip the dead, in my view, not because they must but because holding fast to settled solutions is the best way to give law the predictability and stability it requires, to nail down what we regard as progress, and simply to save ourselves work. The urge to loosen that grip grows stronger with every "next big thing" in warfighting technology, however: "it is never enough to claim a country; it must be held. It must be held and made secure, every generation."[52] The claim that the law doesn't reach *their* conduct will forever be made by scofflaws seeking to evade its reach. That claim is no less repugnant in the realm of cyber rules than elsewhere—but in cyber rules, as elsewhere, that claim must be considered, for in no realm can either lawgivers or law interpreters evade the command of the law to decide what the rules cover and what they do not. The response to a spurious assertion of a gap, therefore, is not to profess that gaps do not exist; the response is to assess whether a particular gap *does* exist and, if not, to enforce the law.

The point, then, is that there *is* a difference between lawmaking and law interpreting; that however hard it is to disentangle the two, it's *possible* that gaps in the law governing cyber conflict can exist; and that given that possibility, classification choices that often have been assumed to present neat dyads in fact present triads. Realistic choices, in international law as else-

---

51. The State Department Legal Adviser appears to have implied that Olympic Games constituted a use of force because the physical consequences of the attack worked the same kind of physical damage that dropping a bomb or firing a missile would have. *See* Koh, *supra* note 21. "*Cyber activities*," he added, "*that proximately result in death, injury, or significant destruction would likely be viewed as a use of force*." *Id.* (emphasis in original). Why *proximate* causation is required is not clear; under traditional analysis, kinetic activity that is the cause-in-fact of death, injury or significant destruction would likely be viewed as a use of force.

52. HILLARY MANTEL, WOLF HALL 255 (2009).

where, entail more than mechanical, on/off, light-switch classification. Realistic lawyers are skeptical of essentialist and foundationalist value claims.[53] Realistic lawyering reflects the genealogy of legal rules, the consequences of one interpretation versus another, the structure of incentives and disincentives that a given interpretation would yield, the political and historical context in which a legal issue arises, the expectations of the parties, the level of compliance that rules actually generate, and a variety of other matters none of which can be captured in neat interpretive algorithms as part of a robotic exercise of categorization. Formalism leaves policymakers scratching their heads in puzzlement when pretended "outcomes" don't actually flow from the forms, from the categories, from the rigorous syllogisms that formalist lawyers lay out for them; exclusive reliance upon the categories masks the real factors on which outcomes inevitably depend. A broader approach, which some have called pragmatism,[54] doesn't purport to be certain, universalist or complete. It acknowledges the law's inevitable indeterminacy and inability to foresee, let alone resolve, every possible future case. It recognizes the inconvenient truth "that existing legal rules themselves can be understood only in the light of ideas and information drawn from outside law. . . ."[55] It accepts the risk of phony assertions of gaps in the law as the price of keeping the law honest, alive and understandable. It counsels against reliance upon past choices that are wrongly claimed to have eliminated the need for future choices.[56] But it does identify, or at least tries to identify, what's really at stake in legal disputes, whether old categories are up to the task of resolving those disputes, and where new categories might be needed. And it doesn't stifle legal reform with specious claims of systemic completeness.

III. THE IMPROBABILITY OF NEW LIMITS

A better way of posing the question that I now proceed to address, therefore, is not "whether gaps in the international rules governing cyber con-

53. GLENNON, *supra* note 41, at 5.

54. For a contemporary version in this context, see *id.* For an earlier, and prescient, exploration of some of the same themes, see SAMUEL VON PUFENDORF, ON THE DUTY OF MAN AND CITIZEN ACCORDING TO NATURAL LAW 108 (James Tully ed., Michael Silverthorne trans., 1991) (1682).

55. Dickinson, *supra* note 1, at 122.

56. *Cf.* HART, *supra* note 28, at 129.

flicts are likely to be filled"; rather, the question is whether States are likely to consent to new law that limits their freedom to use cyber weapons.

Law is a form of cooperation. Certain conditions normally exist when cooperative mechanisms like law emerge and function properly.[57] Actors within the system, for example, are relatively equal. Future dealings are expected. Trust is high. A consensus exists concerning foundational values. The cost of non-cooperation is high. Individual and collective interests align. Underlying social norms reinforce legal norms. Free riders and transgressors are easily spotted and penalized.

For better or worse, however, these and other conditions necessary to promote the emergence and development of legalist constraints are not present in sufficient degree to support further international rules governing cyber conflict—any more than those conditions have been present, in the past, to support the emergence of rules governing clandestine or covert intelligence operations of which cyber activity normally is a part.

When States are equal in capability, the imposition of legal limits freezes in no advantage or disadvantage. Because cyber capabilities are concealed, however, relative capability becomes speculative, leaving States without the ability to evaluate beforehand the apparent advantages and disadvantages that new rules might reify.[58] States will not regulate the pursuit of core security interests based upon speculation (hence the muted international enthusiasm for Russia's proposal for an international cyber weapons

57. Andrew Hurrell has noted that "fundamental differences in religion, social organization, culture and moral outlook . . . may block or, at least, complicate cooperative action." Andrew Hurrell, *Power, Institutions, and the Production of Inequality*, *in* POWER IN GLOBAL GOVERNANCE 33, 36 (Michael Barnett & Raymond Duvall eds., 2005). *See generally* Simon Maxwell, *Why Cooperate?* (paper distributed at Reforming the United Nations Once and for All, World Economic Forum, Davos, Switzerland (Jan. 23, 2004)) (on file with author); Sarah Gillinson, *Why Cooperate? A Multi-Disciplinary Study of Collective Action* (Overseas Development Institute, Working Paper No. 234, 2004), *available at* http://www.odi.org.uk/resources/docs/2472.pdf. Seminal works in this area include COOPERATION UNDER ANARCHY (Kenneth A. Oye ed., 1986); ROBERT AXELROD, THE EVOLUTION OF COOPERATION (1984); and ROBERT O. KEOHANE, AFTER HEGEMONY: COOPERATION AND DISCORD IN THE WORLD POLITICAL ECONOMY (1984).

58. For similar analysis see Jack Goldsmith, *Cybersecurity Treaties: A Skeptical View*, *in* FUTURE CHALLENGES IN NATIONAL SECURITY AND LAW 6 (Peter Berkowitz ed., 2011), *available at* http://media.hoover.org/sites/default/files/documents/FutureChallenges_Goldsmith.pdf ("Offensive cyber weapons are guarded secrets because knowledge about the weapon enables the building of defenses and because revelation about attack capabilities would reveal a lot about exploitation capabilities."). *See also* Jack Goldsmith, *The New Vulnerability*, NEW REPUBLIC, June 7, 2010, at 21.

ban).[59] For similar reasons, customary international rules on these issues are unlikely. Customary international law depends upon connecting dots of historical precedents that form patterns of practice, but States have been disinclined to talk publicly about cyber incidents in which they have been involved.

When future dealings are expected, States confront a greater incentive to come up with a mutually advantageous rule, such as the UN Charter's prohibition against non-defensive use of force. If, however, the sponsor of a cyber attack can't be identified because sponsorship of the attack—or the attack itself—is concealed, as is often true of cyber attacks, then the future casts no shadow and no State need be concerned about future rewards or penalties; law can impose no punishment.

More than anything else, however, it is this element of attributability—the reciprocal ability to say "who did it"—that makes law work. When a transgressor can be identified, penalties can be assessed, and retaliation and deterrence are possible—and so is legal regulation. Attribution permits the target to assign responsibility. It provides the rules' ultimate enforcement mechanism—the ever-present threat of retaliation and punishment. It therefore establishes compliance incentives. And attributability enables legal recourse against transgressors, not only in the International Criminal Court and other international tribunals, but also in the domestic courts of nations that comply with their international obligation to investigate and prosecute war crimes. If cyber activity and its sponsor are concealed, however, and verification of compliance is impossible, so too is deterrence[60] and effective legal regulation. No verifiable international agreement can regulate the covert writing or storage of computer code useful for launching a clandestine cyber attack.

Indeed, this single reciprocal condition—the ability of a target nation to identify and threaten assailants in one way or another—underpins the entire

---

59. *See* U.N. GAOR, Letter dated September 23, 1998 from the Permanent Representative of the Russian Federation to the United Nations to the Secretary General concerning Agenda Item 63, U.N. Doc. A/C.1/53/3 (Sept. 30, 1998).

60. For commentary on deterrence in cyber conflict, see Patrick M. Morgan, *Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm*, *in* COMMITTEE ON DETERRING CYBERATTACKS, NATIONAL RESEARCH COUNCIL, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 55 (2010), *available at* http://www.nap.edu/openbook.php?record_id=12997&page=55; Mike McConnell, *To win the cyber-war, look to the Cold War*, WASHINGTON POST, Feb. 28, 2010, at B1.

legal edifice that regulates armed conflict.[61] The prohibition against aggression is empty absent an ability to ascertain the aggressor. The protection of noncombatants disappears unless the assailant is identifiable. The law of neutrality is meaningless absent an ability to identify a belligerent. The possibility of reprisal or self-defense evaporates absent an ability to know what nation to take measures against. The notion of command responsibility dissolves absent knowledge of who the commander is. In marginal instances States' interests induce compliance with the law of war despite attribution difficulties; compliance sometimes can produce extrinsic benefits for the law-abiding, such as shortening conflicts or stabilizing post-conflict environments even when adversaries flout the law of war. But the modern rules of war are effectively premised on attributability.

Internationally, the reciprocal possibility of identification thus makes violence less likely because it exposes the attacker to risk in three ways. First, retaliation is possible. While the modern laws of war generally prohibit reciprocal violation, in practice the vitality of those rules often has depended upon the threat of retaliation. It would not, for example, have been permissible under international law to use chemical weapons against Nazi Germany in response to its putative use of such weapons, but it is entirely plausible that Hitler exercised restraint because of the credible threat to do so by Roosevelt and Churchill.[62] Second, the identification of transgressors makes remedial legal action possible. For States, penalties for charges of aggression or disproportionate and indiscriminate attacks, for example, can take the form of economic sanctions, reparations or other remedies, as Iraq discovered following its invasion of Kuwait.[63] For individuals, acts perpetrated during periods of armed conflict that transgress the laws of war, such as targeting civilians or torturing adversaries, give rise

---

61. *See* James D. Murrow, *When Do States Follow the Laws of War?*, 101 AMERICAN POLITICAL SCIENCE REVIEW 559, 560 (2007) (describing the role of "reciprocal enforcement" in "[c]ompliance with the laws of war").

62. President Franklin D. Roosevelt warned that any use of poisonous or noxious gases by the enemy would be met by the "fullest possible retaliation":

> [T]here have been reports that one or more of the Axis powers were seriously contemplating use of poisonous or noxious gases or other inhumane devices of warfare. . . . We promise to any perpetrators of such crimes full and swift retaliations in kind. . . . Any use of gas by any Axis power, therefore, will be followed by the fullest possible retaliation upon munition centers, seaports, and other military objectives throughout the whole extent of the territory of such Axis country.

Use of Poison Gas, 8 DEPARTMENT OF STATE BULLETIN 507 (1943).

63. *See* S.C. Res. 661, U.N. Doc. S/RES/661 (Aug. 6, 1990).

to individual criminal responsibility. The war crimes against Bosnian Croat and Muslim civilians during the Bosnian war of the 1990s could not be prosecuted had the alleged perpetrators, such as Radovan Karadžić and Ratko Mladić, not been identified and indicted. Third, identification can impose reputational costs that are not without consequences. More than one prominent American official has escaped formal punishment for the mistreatment of prisoners in recent years but endured widespread denunciation because the chain of command was (at least on occasion) transparent enough to pinpoint responsibility.

Sometimes, of course, those costs are light enough or improbable enough for a transgressor to absorb painlessly. Muammar Gaddafi flouted all legal obligations in his effort to remain in power in Libya, and Syrian President Bashar al-Assad, while attempting to exonerate himself of personal liability, has long seemed undeterred by the possibility of criminal prosecution for crimes against his country's civilians. An effective rule of law ultimately relies on making the costs of non-compliance exceed the costs of compliance; the history of international law has been a struggle to do just that. Anonymity makes violation cost-free, however, because the assignment of responsibility and imposition of penalties are impossible. Attributability, in contrast, creates reciprocity-induced restraints. It produces greater regularity in conflict management, enhanced predictability in inter-State relations and increased systemic stability.

How, then, do the conditions needed for effective international rules affect the amenability of cyber operations to international regulation of cyber weapons and cyber attacks? Cyber operations' "attribution problem,"[64] so-called, in reality exists at three levels. To attribute a cyber attack to a State, it's necessary to establish what computer was used, who was sitting at the computer (if it's not government-owned), and what government or organization that person worked for. Sophisticated cyber attacks of the sort launched by governments normally are extremely difficult to trace at any of those levels. Most experts believe that the possibility of concealment is baked into the structure of the Internet and cannot feasibly be eliminat-

64. *See* Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARVARD INTERNATIONAL LAW JOURNAL 373, 397–408 (2011). For an excellent review of the technological difficulties involved in attribution with regard to cyber operations, see also JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 50–51, 133–34, 234–35 (2011); David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARVARD NATIONAL SECURITY JOURNAL 531 (2011).

ed.[65] Circumstantial evidence and inferred motives have led experts to suspect State involvement in a number of cyber attacks over recent years, but have not provided the level of probability long thought necessary to justify military retaliation.

It remains likely, therefore, that the law of war, compliance with which depends heavily upon attributability and related background conditions, will not be refined to further regulate cyber operations.

The possibility of further regulation cannot be dismissed, however, particularly after the *New York Times* confirmed that the United States and Israel were behind Stuxnet.[66] Policymakers cannot automatically assume deniability, for secrecy is not the only incentive that drives States. Policymakers confront a dilemma: they seek secrecy, of course, for all the reasons that plausible deniability is sought in covert operations; "[n]on-attribution to the United States for covert operations," the Church Committee found, "was the original and principal purpose of the so-called doctrine of 'plausible denial.'"[67] But policymakers at the same time want the world—and often need the world—to know of their successes. They are credit-seeking, blame-avoiding actors. They seek praise for what they do. They don't want to be found at fault if the public in the fullness of time learns that war might have been avoided through the discrete use of some amazing new application like Stuxnet. They want to make their political leaders look tough, their software designers look smart and their nation's adversaries look twice before attacking. All this requires public disclosure—leaks.[68] Attribution, therefore, cannot be masked entirely by computer technology, even if the Internet does remain opaque. No "HAL 9000" runs the

65. *See* Clark & Landau, *supra* note 64, at 531 ("The Internet was not designed with the goal of deterrence in mind. . . ."); *see also* Susan W. Brenner, *"At Light Speed": Attribution and Response to Cybercrime/Terrorism/Warfare*, 97 JOURNAL OF CRIMINAL LAW AND CRIMINOLOGY 379 (2007) (discussing how computing technology complicates attribution); W. Earl Boerbert, *A Survey of Challenges in Attribution*, *in* COMMITTEE ON DETERRING CYBERATTACKS, *supra* note 60, at 41, 41–52, *available at* http://www.nap.edu/openbook.php?record_id=12997&page=41 (outlining the barriers to both technological and human attribution in cyberspace).

66. *See* Sanger, *supra* note 3.

67. SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, INTERIM REPORT: ALLEGED ASSASSINATION PLOTS INVOLVING FOREIGN LEADERS, S. REP. NO. 94-465, at 11 (1975), *available at* http://www.intelligence.senate.gov/pdfs94th/94465.pdf.

68. "That's another of those irregular verbs, isn't it? I give confidential press briefings; you leak; he's being charged under section 2A of the Official Secrets Act." *Yes, Prime Minister: Man Overboard* (BBC television broadcast Dec. 3, 1987).

show—yet—and human involvement is a trapdoor, waiting to be exploited by spies and reporters.

That being true, what lies ahead? The answer depends largely upon the course of future events. At one end of the spectrum lies an overt, immediately attributable cataclysmic cyber shock—a "digital Pearl Harbor" involving, say, a massive, sustained East Coast power outage in midwinter, breaking pipes and disabling ATMs, police communications and air traffic control systems. In that event, pressure would be brought to bear on the U.S. government to take the lead in devising new international rules to prevent a recurrence, much as occurred in 1919 at Versailles and 1945 in San Francisco. At a minimum, new rules could take the form of targeted, universal sanctions directed at wrongdoers; at a maximum one could envision an explicit redefinition of self-defense to permit the use of kinetic force in response to a cyber attack.

At the other end of the spectrum lie "drip-drip" clandestine cyber attacks—an occasional "flash crash" on a stock exchange that no one can explain, a mysterious airline accident here, a strange power blackout there, incidents extending over months or years, with no traceable sponsorship. Although the ultimate cost of these attacks could be great, they are likely to be tolerated because the costs are incurred gradually and incrementally, because no sponsor can be quickly identified[69] and because the countervailing benefits of cyber weapons seem greater by comparison (as with Stuxnet). For a financially strapped and war-weary public and an American military establishment inclined toward "light footprints," those are strong reasons not to bargain away cyber weapons.

In this scenario, cyber weapons research is driven not by adversaries' actual capabilities but by the reciprocal assumption that if we can discover it, an adversary can also discover it—the classic security dilemma that creates an inexorable forward momentum. Cyber operations are in this view

69. As the time required to identify an attacker increases, the likelihood of a forceful response decreases. The Libyan bombing of Pan Am Flight 103 is an example. Confirming the Libyan government's involvement took years, during which the aggrieved States relied upon law enforcement rather than military remedies. Immediate confirmation might have drawn comparisons to the German sinking of the *Lusitania* in 1915, which contributed significantly to U.S. entry into World War I. *See* Jonathan B. Schwartz, *Dealing with a "Rogue State": The Libya Precedent*, 101 AMERICAN JOURNAL OF INTERNATIONAL LAW 553, 555–56 (2007) (describing how the United States and United Kingdom "elected to treat the bombing of Pan Am 103 as a crime under their domestic legal processes" rather than "consider[ing] [it] an 'act of war,' as the United States had treated the Libyan-sponsored attack on off-duty U.S. military personnel at a Berlin nightclub . . . in 1986").

regarded as merely the latest efforts—the latest *successes*—at injecting less risk into combat, merely the most recent in a long history of efforts by States to fight at a greater distance, to afford greater protection to non-combatants (and combatants), to enhance proportionality—in effect, to pursue many of the ends of humanitarian law. States in this scenario will continue to seek concealment but will recognize that the operation is discoverable and attributable. In the recognition of that risk lies the possibility of some international legal regulation. But that regulation, if it occurs, will not likely be deep or broad, because it will be limited by the same incentive structure that drives it: policymakers will continue to seek out rules, here as elsewhere, intended to permit what they're doing but to limit what their adversaries might do. So the blades of such rules are likely to be dull, for the authors' own protection.

How likely is each of those scenarios? The truth is that only a handful of people in the world—if that—are knowledgeable enough to say. I am not one of them. It would be a mistake, however, to underestimate the humanitarian and institutional costs lurking in the seemingly benign, second scenario of drip-drip attacks and counterattacks. If they have anything in common with warriors of the past, cyber warriors will be less inhibited in initiating computer-induced violence. Anonymity, and the distance from violence that provides it, will afford not only safety and insulation against retaliation; distance removes inhibitions against committing acts of violence. Cyber and drone technologies insert greater separation between hunter and victim than ever before: no screams are audible and no blood is visible when pain is inflicted thousands of miles away, merely by hitting the "enter" button on a keyboard.[70] The hunter may not even know whether a "kill" has occurred. In a sequence of relentless cyber attacks and counterattacks, the risk assessment of warfighting is carried out behind closed doors, in the security of Sensitive Compartmented Information Facilities, safely

70. Joshua Greene's research has shown that the thought of killing with one's bare hands is more disagreeable than the thought of killing by throwing a switch that kills from afar. Primates find screams of pain aversive. *See* Joshua D. Greene, *The Secret Joke of Kant's Soul*, *in* 3 MORAL PSYCHOLOGY: THE NEUROSCIENCE OF MORALITY: EMOTION, BRAIN DISORDERS, AND DEVELOPMENT 35, 43 (Walter Sinnott-Armstrong ed., 2008) ("[W]hen harmful actions are sufficiently impersonal, they fail to push our emotional buttons, despite their seriousness, and as a result we think about them in a more detached, actuarial fashion."). For the philosophical origins of the "trolley problem," see Judith Jarvis Thomson, *The Trolley Problem*, 94 YALE LAW JOURNAL 1395 (1985); Philippa Foot, *The Problem of Abortion and Negative and Positive Duty: A Reply to James LeRoy Smith*, 3 JOURNAL OF MEDICINE AND PHILOSOPHY 253 (1978).

immune from legislative or public scrutiny. Cyber attacks, as "sources and methods," are kept secret from Congress. No citizenry is aroused to object. Indeed, the public doesn't even know that an attack has been launched. Which States or terrorists are behind the attacks are—in the public sphere—anyone's guess. Retaliatory attacks, as well as preventive and preemptive attacks, are launched instantaneously, and are thus triggered by an adversary's presumed capability and inferred motives rather than by actual or apparent provocations. As a result, drip-drip strikes—and something very like war—occur more often, in more places, against more targets, based upon weaker evidence.

If that's the road ahead, gaps or no gaps, we are in for a rough ride.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Methods and Means of Cyber Warfare

William H. Boothby

89 INT'L L. STUD. 387 (2013)

Volume 89 2013

Methods and Means of Cyber Warfare

William H. Boothby[*]

I. WHAT IS A CYBER WEAPON?

Central to the conduct of hostilities in an armed conflict are the tools and techniques with which the fight is undertaken. In non-cyber warfare, the tools, that is, the missiles, bombs, rifles, bayonets, mines, bullets and other weapons and associated equipment, are employed in ways that differ according to the military purpose that it is being sought after. These twin ideas of "military tools" and of the ways in which they are employed can be applied equally to cyber warfare. It follows that we should consider how the law that regulates, respectively, the tools or means of warfare and the ways or methods whereby those tools are used should properly be applied in the cyber context.

Any discussion of cyber methods and means of warfare should take as its starting point the more general notion of means and methods of warfare. Means of warfare consist of all weapons, weapons platforms and associated equipment used directly to deliver force during hostilities. Methods of warfare consist of the ways in which weapons are used in hostilities.

Weapons are devices, munitions, implements, substances, objects or pieces of equipment which generate an offensive capability that can be ap-

* Air Commodore, Royal Air Force (Ret.).

plied to an enemy person or object.[1] The *Manual on the Law of Air and Missile Warfare* (*AMW Manual*) defines the term "weapon" as "a means of warfare used in combat operations, including a gun, missile, bomb or other munitions, that is capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of, objects."[2] The accompanying commentary makes the point that the force used need not be kinetic, citing the effects produced by certain computer network operations.[3] In its Glossary of Military Terms, the U.S. Department of Defense defines a weapon system as "[a] combination of one or more weapons with all related equipment, materials, services, personnel, and means of delivery or deployment (if applicable) required for self-sufficiency."[4] The *AMW Manual* characterizes "means of warfare" as "weapons, weapon systems or platforms employed for the purposes of attack"[5] with the result that means of warfare involves not just weapon systems, but also equipment used to control, facilitate or direct the conduct of hostilities.[6]

Weapons as conventionally understood can take a variety of forms. While some weapons, such as bombs, rockets, bullets, artillery shells and the like generate their destructive effect by the use of kinetic force, other kinds of weapons, such as gases, chemical and biological agents achieve

1. WILLIAM H. BOOTHBY, WEAPONS AND THE LAW OF ARMED CONFLICT 4, 344 (2009).

2. PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE rule 1(ff) (2009). The Program on Humanitarian Policy and Conflict Research at Harvard University (HPCR) convened a group of international legal experts to review and restate the existing law of air and missile warfare. At the end of a multi-year process HPCR published the *Manual on International Law Applicable to Air and Missile Warfare*, which contains the black-letter rules reflecting the overall consensus of the legal experts of the existing law of international armed conflict bearing on air and missile warfare. HPCR also published the COMMENTARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE (2010) [hereinafter AMW COMMENTARY]. In the *Commentary* each Black-letter Rule is accompanied by a commentary intended to provide explanations of the rule. For ease of citation, citations in this article will be to the *Commentary* since it contains both the rules and their associated commentary.

3. AMW COMMENTARY, *supra* note 2, rule 1(ff) cmt. ¶ 1, at 55.

4. Joint Chiefs of Staff, Joint Publication 1-02, DOD Dictionary of Military and Associated Terms (Nov. 8, 2010), as amended through July 15, 2012, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

5. AMW COMMENTARY, *supra* note 2, rule 1(t), at 41.

6. *Id.*, rule 1(ff) cmt. ¶ 3, at 55.

their wounding or deadly purpose without necessarily operating kinetically.[7] The critical factor in relation to all weapons is the injurious or damaging effect that they have on the persons and/or objects associated with the adverse party to the conflict.

Applying these notions in the cyber domain, the immediate question is how a cyber capability resident, for example, on a thumb drive that is released by simply pressing the "enter" key can possibly be described as an offensive capability, thus, potentially, as a cyber weapon. As Professor Schmitt has pointed out, it is the violent consequences that are designed or intended to follow the use of the cyber capability that are critical to the characterization of such a cyber event as a cyber attack. The same intended violent consequences are critical to the characterization of a cyber capability as a cyber weapon.[8] Therefore, a cyber weapon would comprise any computer equipment or computer device that is designed, intended or used, in order to have violent consequences, that is, to cause death or injury to persons or damage or destruction of objects.

"Object" denotes any physical object, such as a piece of computing equipment. If the cyber capability burns out components in the targeted computer system, the requirement as to damage will be satisfied. Equally, the effect of the cyber capability on the facility which the targeted computer serves may render the capability a cyber weapon. For example, the object against which the cyber operation is directed is the supervisory control and data acquisition system that controls the operation of a public utility installation, such as a water treatment works, or, a similar computer system that controls a production process, such as at an oil refinery. In these cases the damage that is caused by the cyber operation to the water treatment installation or to the oil refinery will also cause the cyber tool to be considered a cyber weapon.

The next question is whether damage to data within a computer system that does not affect the facility or service that the targeted computer system provides constitutes damage for these purposes. In other words, is the data resident in the target computer system to be regarded as an object? The author's view is that such data only becomes an "object" when it is critical

7. While it is well appreciated that the listed weapons are generally prohibited by treaty, it is the fact that they are nevertheless widely recognized as weapons that is critical here.

8. Michael N. Schmitt, *Cyber Operations and the* Jus in Bello*: Key Issues*, *in* INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 89, 93–94 (Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies).

to the operation of the targeted system.[9] If as a result the targeted computer ceases to perform the required control function causing, in our examples, water purification or oil refining to cease, this would amount to damage if repairs are needed before production can resume. A cyber tool being used for such a purpose would, therefore, be a cyber weapon. Temporary shutdown causing inconvenience or irritation would not amount to damage or injury, and use of a cyber tool to cause those results would not cause it to be regarded as a cyber weapon.[10]

If, in considering these principles, we conclude that a particular cyber tool has an offensive capability, the remaining issue is whether it can properly be described as "applied" to an enemy person or object. There is an inherent indirectness about cyber activity in which there are often numerous orders of effect. The first order of effect is the direct impact of the cyber activity on the data in the targeted computer. That produces the second order effect by affecting the service the target computer provides. The resulting damage, injury and other consequences that the termination or interruptions of service cause to the customers of the targeted computer system constitute third order effects, which may well have been the main purpose in undertaking the cyber operation. Computer linkages and customer dependencies taken together comprise the mechanism that is being exploited to apply the offensive cyber capability—or cyber tool—to the targeted object or person. Indeed, that cyber tool can properly be regarded as applied to all of the devices, data, objects and persons within this chain of effect.

We can therefore properly conclude that computers, computer data and associated mechanisms that are capable of generating any of these orders of effect on an adverse party to the conflict are capable of being a cyber weapon. Such computers, data or mechanisms will only actually become a cyber weapon, however, if they are used, designed or intended to be used for such purposes.[11]

---

9. *See also* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE rule 38 cmt. ¶ 5 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

10. For a discussion of these issues in relation to the notion of cyber attack, see KNUT DÖRMANN, APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS 6 (2004), *available at* http://www.icrc.org/web/eng/siteeng0.nsf/htmlall/68lg92?opendocument (paper delivered at the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm); Schmitt, *supra* note 8, at 95.

11. A distinction must therefore be drawn between the use of cyber capabilities for offensive purposes, as discussed in this section of the article, and their use, for example,

II. FUNDAMENTAL PRINCIPLES OF WEAPONS LAW

The customary, fundamental principles and established rules of weapons law apply to cyber weapons no less than any other weapons. As the International Court of Justice observed in the *Nuclear Weapons* advisory opinion,

> the intrinsically humanitarian character [of the established principles and rules of humanitarian law applicable in armed conflict] permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future.[12]

There are three customary principles of weapons law. The first is that the right of the parties to an armed conflict to choose methods or means of warfare is not unlimited.[13] This means that those involved in undertaking cyber operations during armed conflicts have a clear legal duty to "respect the rules of international law applicable in case of armed conflict."[14]

By the second customary principle, it is "prohibited to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering."[15] The injury and suffering to

---

for information gathering or espionage. While a cyber capability may be capable of generating the stated orders of effect, thereby causing death, injury, damage or destruction, it is only if it is used to cause these things that it will become a weapon. While the logic leading to this conclusion seems to the author to be inescapable, consider, however, the valid issues raised in Duncan Blake & Joseph S. Imburgia, *Bloodless Weapons? The Need to Conduct Legal Reviews of Certain Capabilities and the Implications of Defining Them as "Weapons,"* 66 AIR FORCE LAW REVIEW 157 (2010).

12 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 86 (July 8), *reprinted in* 35 INTERNATIONAL LEGAL MATERIALS 809 (1996).

13. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 35(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

14. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 1404 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987). Note also the Martens clause at Additional Protocol I, art. 1(2), *supra* note 13 ("In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.").

15. Additional Protocol I, *supra* note 13, art. 35(2). The original U.S. Department of Defense weapons review directive was prepared by Edward R. Cummings, Waldemar A. Solf and Harry Almond. They included in the document what the author regards as the most clear and accurate formulation of the superfluous injury and unnecessary suffering

be assessed in the case of cyber weapons is that expected under each of the orders of effect that were described in the previous section. In applying this rule, the legitimacy of a cyber weapon must be assessed "by comparing the nature and scale of the generic military advantage to be anticipated from the weapon in the application for which it is designed to be used with the pattern of injury and suffering associated with the normal, intended use of the weapon."[16] The references to the generic nature of the military advantage and to the injury and suffering associated with normal use make the point that this test is mainly concerned with the generality of such aspects and not with the circumstances on a particular occasion. It is the qualities of the weapon per se, rather than the particularities of a specific attack, with which the weapons law test is usually concerned. If, however, as will frequently be the case, a cyber weapon is being prepared or procured in order to be used on a known occasion against a specified target, the ad hoc circumstances must be carefully considered when determining whether the superfluous injury/unnecessary suffering test is satisfied.[17]

---

test currently available. The test is lengthy but is reproduced here because of its clarity and relevance.

> The prohibition of unnecessary suffering constitutes acknowledgment that necessary suffering to combatants is lawful, and may include severe injury or loss of life. There is no agreed international definition for unnecessary suffering. A weapon or munition would be deemed to cause unnecessary suffering only if it inevitably or in its normal use has a particular effect and the injury caused is considered by governments as disproportionate to the military necessity for it, that is, the military advantage to be gained from its use. This balancing test cannot be conducted in isolation. A weapon's or munition's effects must be weighed in light of comparable, lawful weapons or munitions in use on the modern battlefield. A weapon is not unlawful merely because it may cause severe suffering or injury. The appropriate determination is whether a weapon's or munition's employment for its normal or expected use would be prohibited under some or all circumstances. The correct criterion is whether the employment of a weapon for its normal or expected use inevitably would cause injury or suffering manifestly disproportionate to its military effectiveness.

This text is reproduced in W. Hays Parks, *Means and Methods of Warfare,* 38 GEORGE WASHINGTON INTERNATIONAL LAW REVIEW 511, 517 n.25 (2006). *See also* MICHAEL BOTHE, KARL JOSEF PARTSCH & WALDEMAR A. SOLF, NEW RULES FOR VICTIMS OF ARMED CONFLICTS, COMMENTARY ON THE TWO 1977 PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 1949, at 200–201 (1982).

16. William J. Fenrick, *The Conventional Weapons Convention: A Modest but Useful Treaty*, 279 INTERNATIONAL REVIEW OF THE RED CROSS 498, 500 (1990); BOOTHBY, *supra* note 1, at 63.

17. Accordingly, when a cyber weapon is being developed for use against a known target, it is the injury to persons that is to be expected as a result of the way it is to be used on that occasion against the intended target that must be compared with alternative methods of achieving the desired military purpose in order to determine whether the cyber

The third customary principle of weapons law is that it is prohibited to employ weapons, means or methods of warfare, including cyber weapons, which are indiscriminate by nature. This rule, derived from Article 51(4) of the 1977 Additional Protocol I (AP I) to the four 1949 Geneva Conventions, has customary law status, thus binding all States.[18] If the cyber weapon cannot be directed at a particular military objective or if its effects cannot be controlled, it will likely breach this weapons law part of the discrimination rule.[19]

This rule would seem to be particularly relevant to cyber weapons. Thus, if the characteristics of a piece of cyber malware are such that it will cause damage to the target computer system, but also infect and damage numerous other civilian computer systems or websites, the cyber weapon may be indiscriminate by nature and prohibited by the rule. The critical issue here is whether the cyber weapon not only engages the intended target, but also reasonably limits its damaging effect to that intended target.

An attack that breaches the proportionality rule in Article 51(5)(b) of AP I is an example of an attack that would breach the indiscriminate attacks prohibition.[20] In the cyber context, it will not be the only example.

---

weapon, means or method of warfare is of a nature to cause superfluous injury or unnecessary suffering.

18. Having noted that indiscriminate attacks are prohibited, the paragraph so far as relevant, defines indiscriminate attacks as

> (b) those which employ a method or means of combat which cannot be directed at a specific military objective; or (c) those which employ a method or means of combat the effects of which cannot be limited as required by [the] Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

Additional Protocol I, *supra* note 13, art. 51(4). The V2 rockets used by Germany towards the end of World War II are the sort of weapon that would have breached this rule. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 14, ¶ 1958. On the rule generally, see Michael N. Schmitt, *Future War and the Principle of Discrimination*, 28 ISRAEL YEARBOOK ON HUMAN RIGHTS 51, 55 (1998).

19. The UK *Manual* observes, "It is prohibited to employ weapons which cannot be directed at a specific military objective or the effect of which cannot be limited as required by Additional Protocol 1 and consequently are of a nature to strike military objectives and civilians or civilian objects without distinction." UNITED KINGDOM MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 6.4 (2004) [hereinafter UK MANUAL].

20. Article 51(5)(b) of Additional Protocol I provides that the following type of attack is to be considered indiscriminate, namely an attack "which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination

Other examples may include worms, viruses and other malware whose nature is to spread their effects uncontrollably, and cyber malware that, though it is designed to attack only the targeted computer node, is also of a nature to cause incidental second and/or third order damage to civilian users[21] of the target computer system, including those who may not necessarily be known to the targeteer.

The execution of discriminating cyber attacks therefore presupposes that the weapon system to be employed is capable of reasonably limiting its effects to the target computer system and to the targeted customers of that system. This is the first matter to consider when determining whether the cyber weapon is indiscriminate by nature. If it passes that test, the planned operational procedures must adequately inform the assessment whether any particular planned attack will be discriminating. Information will be required as to the target system, its linkages, its dependencies and its customers and as to the customers of any linked system that is also liable to be affected by planned cyber attacks. Planning such attacks will place considerable demands on intelligence resources. Additionally, as will be addressed in the weapons review section below, the reviewer conducting the required legal review will wish to be satisfied that the broader context in which the cyber weapon will be used is not such as to render its nature indiscriminate.

III. SPECIFIC WEAPONS LAW RULES OF RELEVANCE TO CYBER WEAPONS

Some of the technology-specific weapons law rules would seem to be of particular potential relevance to cyber warfare; these are discussed in this section.

Two sets of rules protect the natural environment during armed conflict. Article 35(3) of AP I prohibits the employment of "methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment."[22] By contrast,

---

thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."

21. The word "users" is here intended to include not only persons but systems or objects that would suffer injury, death, damage or destruction.

22. Note that Article 55 of Additional Protocol I additionally requires that care be taken in warfare to protect the natural environment against widespread, long-term and severe damage, such protection to include a prohibition "of the use of methods or means of warfare which are intended or may be expected to cause such damage to the natural environment and thereby to prejudice the health or survival of the population."

the 1976 UN Environmental Modification Convention[23] addresses the use of the environment as a weapon. Its core provision is an undertaking by States party "not to engage in military or any other hostile use of environmental modification techniques having widespread, long-lasting or severe effects as the means of destruction, damage or injury to any other state party."[24] The Convention defines "environmental modification techniques as "any technique for changing—through the deliberate manipulation of natural processes—the dynamics, composition or structure of the Earth, including its biota, lithosphere, hydrosphere and atmosphere, or of outer space."[25]

The effect of these rules is that any cyber weapon, the second and third order effects of which can be expected to be widespread, long-term and severe damage to the natural environment, will be prohibited and should not be used. Equally, the use of cyber methods alone, or perhaps more likely in association with the use of a conventional weapon or substance of some type, to achieve the defined forms of environmental modification and which cause injury, damage or destruction to an opposing party to the conflict is also prohibited. A cyber weapon designed to cause the core of a nuclear electricity generating station to ignite, thereby spreading high levels of long-lasting nuclear contamination that renders wide areas of surrounding territory uninhabitable for very protracted periods, is likely to be an example of a cyber weapon that would breach the AP I rule.

The use of poisons, poisoned weapons and asphyxiating gases is prohibited at customary law and by treaty provision.[26] Biological weapons are

---

23. Convention on the Prohibition of Military or Any Hostile Use of Environmental Modification Techniques, May 18, 1977, 31 U.S.T. 333, 1108 U.N.T.S. 151 [hereinafter ENMOD Convention] For a discussion of ENMOD, see Arthur H. Westing, *The Environmental Modification Convention of 1977—Reflections in Anticipation of the Second Review Conference*, 5 HUMANITÄRES VÖLKERRECHT INFORMATIONSSCHRIFTEN 70 (1992); ENVIRONMENTAL WARFARE: A TECHNICAL, LEGAL AND POLICY APPRAISAL (Arthur H. Westing ed., 1984); Jozef Goldblat, *The ENMOD Convention: A Critical Review*, 2 HUMANITÄRES VÖLKERRECHT INFORMATIONSSCHRIFTEN 82 (1993).

24. ENMOD Convention, *supra* note 23, art. I(1).

25. *Id.*, art. II(1).

26. The customary prohibition on the use of poison and poisoned weapons is reflected in Article 23(a) of the 1907 Hague Regulations. Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2227. *See also* UK MANUAL, *supra* note 19, ¶ 6.19.1; 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW rule 72 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005). The prohibition of the use of asphyxiating gases is set out in the 1925 Geneva Gas Protocol and is binding as customary law.

prohibited by the 1972 Biological Weapons Convention[27] and chemical weapons are prohibited by the 1993 Chemical Weapons Convention.[28] The possession or use of biological weapons is, in the author's view, prohibited by customary law, while the prohibition on use of chemical weapons is fast becoming a customary rule, if indeed it has not already achieved that status.[29] A cyber weapon will not generally have the nature of a poison, gas, chemical or biological weapon. However, cyber operations may enable a party to the conflict to gain effective control over such weapons or substances from an adverse party to the conflict. If a State's use of cyber methods results in it gaining control of poisons, poisoned weapons, asphyxiating gas, chemical weapons or biological weapons from an opposing party, it may not employ cyber or other methods to use such weapons or substances in connection with the armed conflict. It must take action to safeguard and, in the case of chemical and biological weapons, to destroy them to the extent that its degree of control and other factors enable it practically to do so.[30]

Protocols adopted under the aegis of the Convention on Certain Conventional Weapons (CCW)[31] address a number of classes of weapon. Protocol I prohibits weapons "the primary effect of which is to injure by fragments which in the human body escape detection by X-rays."[32] It

---

Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925**,** 26 U.S.T. 571, *reprinted in* 14 INTERNATIONAL LEGAL MATERIALS 49 (1975).

27. Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Apr. 10, 1972, 26. U.S.T. 583, 1015 U.N.T.S. 163 [hereinafter Biological Weapons Convention]. For a discussion of the convention, see Josef Goldblat, *The Biological Weapons Convention—An Overview*, 318 INTERNATIONAL REVIEW OF THE RED CROSS 251 (1997).

28. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Jan. 13, 1993, 1974 U.N.T.S. 45.

29. See discussion in BOOTHBY, *supra* note 1, at 129, 137.

30. Note that the destruction obligations in the Biological Weapons Convention extend to weapons that a State party to the treaty possesses or controls. Biological Weapons Convention, *supra* note 27, art. II. It will be a matter of interpretation whether cyber operations have the effect of placing chemical or biological weapons under the control of a State party to the relevant Convention. If they do have that effect, the obligations in the relevant Convention addressed to a State having control of such a weapon must be considered.

31. Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Oct. 10, 1980, 1342 U.N.T.S. 137.

32. Protocol on Non-Detectable Fragments, Oct. 10, 1980, 1342 U.N.T.S. 168.

would seem most unlikely that a cyber weapon would be designed or intended to have a second or third order effect of releasing a weapon with such characteristics. Protocol II and the amended version of the Protocol will be considered below. Protocol III[33] imposes prohibitions and restrictions on the use of incendiary weapons as defined in Article 1 of the Protocol. It is prohibited to make a military objective located within a concentration of civilians the object of attack by air-delivered incendiary weapons. A similarly located military objective may only be made the object of attack by a non-air-delivered incendiary weapon if the military objective is clearly separated from the concentration of civilians, and all feasible precautions are taken to limit the incendiary effects to the military objective and avoid or minimize incidental civilian injury and loss.

Protocol IV[34] to the CCW prohibits laser weapons specifically designed as one of their combat functions to cause permanent blindness to unenhanced vision.[35] If a laser weapon has the potential to cause such blindness, it would be unlawful to use in conjunction with that weapon a cyber tool that is intentionally designed to cause permanent blindness. For example, a cyber tool designed to direct the laser beam towards the line of sight of enemy personnel would be prohibited.

Mines[36], booby-traps[37] and other devices[38] are regulated by Protocol II[39] and Amended Protocol II to the CCW. Anti-personnel mines are prohibit-

---

33. Protocol on Prohibitions or Restrictions on the Use of Incendiary Weapons, Oct. 10, 1980, 1342 U.N.T.S. 171.

34. Protocol on Blinding Laser Weapons, Oct. 13, 1995, 1380 U.N.T.S. 370.

35. *Id.*, art. 1. Article 4 defines permanent blindness.

36. "'Mine' means a munition placed on, under or near the ground or other surface area and designed to be exploded by the presence, proximity or contact of a person or vehicle." Amended Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices art. 2(1), May 3, 1996, 2048 U.N.T.S. 93 [hereinafter CCW Amended Protocol II].

37. "'Booby-trap' means any device or material which is designed, constructed or adapted to kill or injure and which functions unexpectedly, when a person disturbs or approaches an apparently harmless object or performs an apparently safe act." *Id.*, art. 2(4).

38. "'Other' devices means manually emplaced munitions and devices including improvised explosive devices designed to kill, injure or damage and which are actuated manually, by remote control or automatically after a lapse of time." Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices art. 2(3), Oct. 10, 1980, 1342 U.N.T.S. 168 [hereinafter CCW Protocol II]. Note the developed definition of the same term for the purposes of Amended Protocol II, namely, "'Other devices' means manually-emplaced munitions and devices including improvised explosive devices de-

ed by the 1997 Ottawa Convention.[40] The references to "exploded" and to munition placement in the CCW mine protocols lead to the common sense conclusion that a purely cyber weapon cannot be a mine. For similar reasons, a purely cyber weapon cannot be an anti-personnel landmine within the meaning of the Ottawa Convention.[41]

However, the CCW Protocol II definition of booby-trap refers to "any device or material," notions that would seem to be broad enough potentially to include a cyber device. If a cyber device were, for example, to take the form of a kill switch embedded in a piece of malware planted by cyber means into the target computer system and which operates unexpectedly when a user of the targeted computer system undertakes a usually safe task such as switching on the computer, there is the potential for the cyber device to come within the Protocol II definition of booby-trap.[42] The cyber device is only capable of being a booby-trap, however, if it is "designed, constructed or adapted to kill or injure." If malware comprising a kill switch is designed to disable, say, the electricity supply to facilities that are essential to life support, it would be a matter of national interpretation whether this amounts to designed, constructed or adapted to kill or injure. While death or injury may be the intended second or third order effect of such a device, States may take the view that only devices that kill or injure as the immediate, or first order effect, come within the Protocol II definition. A less restrictive view would, however, see certain cyber capabilities as coming within the definition of booby-trap, with the result that Articles 3, 7, 9 to 14 and elements of the Technical Annex to the treaty would apply to such cyber weapons.[43] Article 7 would specifically prohibit the use of such booby-traps in any way associated with the objects listed in paragraph (1).[44]

---

signed to kill, injure or damage and which are actuated manually, by remote control or automatically after a lapse of time." CCW Amended Protocol II, art. 2(5).

39. CCW Protocol II, *supra* note 38.

40. Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction, Sept. 17, 1997, 2056 U.N.T.S. 211.

41. *Id.*, art. 2 (defines anti-personnel mines as meaning mines "designed to be exploded" by specified events).

42. TALLINN MANUAL, *supra* note 9, rule 44.

43. A similar definition of booby-trap appears in Article 2(2) of CCW Amended Protocol II. A State party that takes the view that a cyber weapon comes within the definition would apply Articles 3, 4 and 6–9.

44. The listed objects are internationally recognized protected emblems, signs or signals; sick, wounded or dead persons; burial or cremation sites or graves; medical facilities,

The Protocol II definition limits "other devices" to "manually emplaced munitions and devices." This would seem to exclude devices that are emplaced by remote means, such as by email. If, however, a thumb drive bearing the malware were to be manually inserted into the target computer system, it would be a matter of national interpretation whether this amounts to "manual emplacement" for the purposes of Protocol II and Amended Protocol II. It may be reasonable for States to conclude that the cyber weapon is distinct from the gadget that is used to transport it, and to decide that the thing being manually emplaced is the thumb drive, as opposed to the cyber weapon that it contains. Such an approach would suggest that a cyber weapon is not capable of being an "other device" for the purposes of those treaties.[45]

If a State's use of cyber methods enables it to take control of minefields, booby-traps or "other devices" from an opposing party, it may only use such weapons in accordance with the relevant treaty rules to which it is subject. If, however, a computer control system associated with a minefield, booby-trap or other device were to be transferred into the control of another party to the conflict as a result of a cyber operation, it would be a matter of interpretation whether that party had a sufficient degree of control over them for the Protocol II, Amended Protocol II and/or Ottawa Convention obligations to arise.

Where cluster munitions are concerned, a State that is party to the Convention on Cluster Munitions[46] and which, by cyber means, takes control of the cluster munitions of an adverse party to the conflict may not use such cluster munitions in breach of its own treaty obligations. It must also take action to safeguard and destroy them to the extent that its degree of control and other factors make it practicable to do so.

---

medical equipment, medical supplies or medical transportation; children's toys or other portable objects or products specially designed for the feeding, health, hygiene or clothing or education of children; food or drink; kitchen utensils or appliances except in military establishments, military locations or military supply depots; objects clearly of a religious nature; historic monuments, works of art or places of worship which constitute the cultural or spiritual heritage of peoples; or animals or their carcasses.

45. The corresponding definition in Article 2(3) of CCW Amended Protocol II is expressed in similar, but not identical, terms so it would be equally respectable to conclude that a cyber weapon is not capable of being an "other device" for the purposes of the amended Protocol.

46. Convention on Cluster Munitions, *opened for signature*, Dec. 3, 2008, *reprinted in* 48 INTERNATIONAL LEGAL MATERIALS 357 (2008). "Cluster munition" is defined by Article 2 of the Convention.

The discussion in this section is not intended to be an exhaustive treatment of all of the rules of weapons law that may potentially be of relevance in the cyber context. Rather it is intended to illustrate how cyber activity may either constitute activity that is covered by a weapons law provision or may, because of the control being exercised over an adverse party's weapon, give rise to weapons law responsibilities that may not have been foreseen.

IV. WEAPONS REVIEWS OF CYBER WEAPONS

The determination that certain cyber capabilities constitute weapons leads to the inescapable conclusion that they require legal review. While all States are legally obliged, as a matter of customary law, to "ensure that the means of cyber warfare that they acquire or use comply with the rules of the law of armed conflict,"[47] Article 36 of AP I requires that

> in the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[48]

The customary law obligation to review new weapons follows from the general obligation of States to comply with their weapons law duties.[49]

Of the relatively few States that are known to have systems for such review, the UK and U.S. systems, and those in Belgium, Canada, Australia, the Netherlands, Norway, France and Sweden, take the form of a generic

47. TALLINN MANUAL, *supra* note 9, rule 48(a).

48. Rule 48(b) of the *Tallinn Manual* applies this treaty rule specifically to cyber means and methods of warfare.

49. Consider the liability, in appropriate circumstances, to pay compensation in the event of violations of the law of armed conflict in Article 3 of Convention No. IV Respecting the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2227 and Article 91 of Additional Protocol I. Consider also International Committee of the Red Cross, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare, Measures to Implement Article 36 of Additional Protocol I of 1977*, 88 INTERNATIONAL REVIEW OF THE RED CROSS 931, 935 (2006) [hereinafter ICRC Guide]; W. Hays Parks, *Conventional Weapons and Weapons Reviews*, 8 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 55, 57 n.6 (2005). The customary law prohibition of weapons of a nature to cause superfluous injury or unnecessary suffering seems to imply an obligation to assess new weapons by reference to that standard.

review of the weapon in the light of its intended circumstances of use. The review is undertaken before the weapon is released to the armed forces for use in armed conflict.[50] The AP I, Article 82[51] targeting advice to commanders that is provided ad hoc with regard to planned attacks is generally regarded as distinct from the weapon review. Thus, before a non-cyber weapon has been released to the armed forces for employment in combat, commanders will know that it has been the subject of legal review and that the designed or intended use of it, as determined at the time of procurement, accords with the State's international law obligations.

There are, however, characteristics peculiar to cyber weapons that will make the giving of weapons law advice at the development or procurement stage difficult to achieve. A cyber weapon may at that point be so generic in nature that the giving of any meaningful advice as to its compliance with international law becomes speculative. The very nature of the weapon as discriminate or otherwise, and the nature and extent of the generic injury and suffering it will cause, may fundamentally depend on the nature, linkages, dependencies and customer base of the target computer system. In such circumstances, realistic weapons law advice can only be given when those variables are known. This has two obvious consequences. The first is that the operational commander contemplating use of such a weapon may not know in advance that the weapon will be lawful in the circumstances of the use that he intends. The second, consequent on the first, is that the lawyer fulfilling the Article 82 duty to advise a commander with respect to a planned cyber attack may need to build both weapons law and targeting law aspects into his legal advice to the commander.

The weapons law part of such ad hoc advice to the commander will therefore need to consider the context of the attack; the first, second and third order effects that the weapon is expected to produce; the collateral damage expected to civilian users of the target computer system; and whether the nature of the cyber weapon is such as to enable the injury or damage to be restricted to the military objective. In such circumstances, it is obvious that the weapons law advice and the targeting law advice will tend to merge. Even the weapons law assessment of whether the weapon is

50. *See* ICRC Guide, *supra* note 49, at 934.

51. The High Contracting Parties at all times, and the Parties to the conflict in time of armed conflict, shall ensure that legal advisers are available, when necessary, to advise military commanders at the appropriate level on the application of the Conventions and [the] Protocol and on the appropriate instruction to be given to the armed forces on this subject.

capable of being used discriminately and in compliance with the superfluous injury/unnecessary suffering principle will be eclipsed by the issue of whether the planned attack, taking into account the cyber weapon to be used, the circumstances of the target system and of any other nodes liable to be affected, will comply with the customary law targeting rules, and for States party to AP I, with Articles 48 to 67. While this is appreciated, nevertheless, the ad hoc weapons law issues discussed in this article must also be considered, if only to conclude that they have no relevance to the particular circumstances.

Perhaps the safest way forward is for a legal review of all cyber weapons to continue to be undertaken at the weapon development stage. Such reviews can be used to inform the concept of use and associated documents in which the requirement for ad hoc weapons law advice concerning particular types of attack can be noted. Advisers to commanders must, however, appreciate that when advising on planned cyber attacks, a wider range of issues will need to be considered for the reasons set out earlier.

V. APPLYING WEAPONS LAW TO PARTICULAR TYPES OF CYBER WEAPONS

Consideration will now be given to how the weapons law previously discussed can be applied to particular kinds of cyber tools. For these purposes, on an illustrative basis, the use of botnets to deny the services of a targeted computer system, the planting of a kill switch and masquerade will be examined.

Malware might be used to take control of a number of infected computers that become a virtual network centrally controlled by command and control servers. Spam messages are then, for example, sent to the targeted computer system, the bandwidth of which is exhausted, thus prompting the denial-of-service from the targeted system that was the goal of the cyber operation. The malware will cause resources of the infected computers in the net, or bots as they are known, to be devoted to the operation so services to the customers of those systems may also be affected. However, the denial or deterioration of service will only last as long as the botnet is operated and there will normally be no lasting effect on the targeted system. The effect on the targeted computer system will not, therefore, amount to "damage" such that the botnet tool will not thereby be rendered a weapon. If, however, as an example, the targeted system provides life support services that when interrupted will foreseeably cause death or injury, such a use of the cyber tool would render it a weapon requiring legal review.

In conducting that review, the rules of weapons law discussed in this article should be applied. The nature and degree of the injuries suffered and to be expected as a result of such a cyber attack will determine whether the superfluous injury/unnecessary suffering rule has been complied with. More problematic may be the prohibition of cyber weapons that are indiscriminate by nature. It is, however, only death, injury, damage or destruction to protected persons or objects that should be considered. Inconvenience or annoyance caused, for example, by collateral denials-of-service from computer systems forming the botnet will not cause the cyber tool to be indiscriminate by nature.

The use of a targeted Trojan to plant a kill switch involves sending customized—typically concealed—malware to an unaware individual. That individual, by running an apparently safe program or computer file, unknowingly infects the receiving computer system with malware comprising a kill switch. The malware enables the cyber attacker to take control of the target computer system giving him access to all the data stored there. The kill switch can, for example, disable operating programs, corrupt data or close down the target computer system either in response to a command from the cyber attacker or when the authorized operator performs some routine operation, such as switching on the computer. When reviewing such a cyber tool under weapons law, the superfluous injury/unnecessary suffering rule will only need to be considered if the cyber tool, in its intended circumstances of use, is designed or intended to cause injury or death. In deciding whether, when used as intended, the cyber tool is indiscriminate by nature, the designed or intended consequences of activating the kill switch will be critical. Similar considerations to those discussed in the previous paragraph will arise. If the kill switch is designed or adapted to cause death or injury, legal reviewers from states that are party to Protocol II and/or Amended Protocol II to the CCW will consider whether, according to their State's interpretation, such a device amounts to a booby-trap for the purposes of those treaties. Similarly, if the malware containing the kill switch is to be applied to the target computer manually, for example by means of a thumb drive, and if the device is designed to kill, to cause injury or to damage property, the legal reviewer should consider his State's understanding of the definition of "other device" in Protocol II and Amended Protocol II.[52] If the kill switch is to be actuated by remote control, for ex-

52. CCW Protocol II *supra* note 38, art. 2(3) and CCW Amended Protocol II, *supra* note 38, art. 2(5).

ample by a command from the cyber attacker, or if it will activate automatically after a specified time period has elapsed, then the requirements of both Protocols concerning "other devices" will potentially apply to the cyber weapon. If the kill switch is designed to be actuated by a manual act, the provisions of Amended Protocol II relating to "other devices" will potentially apply to the weapon. Here again, much will depend on the relevant State's interpretation of the word "manually." The author considers that, when considered in the context of the Protocols as a whole, "manually" implies a degree of physical connection between the actor and the device which is likely to be absent in the stated example. This is because, in the example, the physical connection is between the actor and the thumb drive, not the device as such.

Masquerade, as a cyber operation, involves the creation of a computer system that mimics the targeted computer system. Customers of the targeted system are diverted to the masquerade system or site where the visiting computer may be infected or where deliberately wrong messages may be given. Clearly, such a cyber tool can be used for a variety of deception-based operations, some of which would be unlawful.[53] Cyber capabilities used for deception-based operations that do not result in death, injury, damage or destruction do not, however, constitute weapons, means or methods of warfare. It is only, therefore, when the masquerade operation is designed or intended to cause death, injury or damage that the cyber tool becomes a cyber weapon requiring legal review. The legal principles prohibiting weapons of a nature to cause superfluous injury/unnecessary suffering or to be indiscriminate will then apply to the masquerade operation. Thus, for example, if the lethal, injurious or damaging effects of the malware cannot be controlled or limited reasonably to military objectives, the cyber weapon is liable to be considered indiscriminate by nature.

53. Consider, for example, the AP I prohibition on causing death, injury or capture by resort to perfidy (Article 37), the prohibition on making improper use of the distinctive emblems (Article 38(1)), the prohibition of unauthorized use of the United Nations emblem (Article 38(2)), the prohibition on using flags, emblems or insignia of neutrals (Article 39(1)) and the prohibition on using flags, military emblems, insignia or uniforms of adverse parties during attacks or in order to shield, favor, protect or impede military operations (Article 39(2)).

VI. CONCLUDING REMARKS

As these illustrations demonstrate, distinctions between the law of weaponry and the law of targeting that have considerable logic when applied to traditional kinetic weapons are more difficult to maintain in the cyber context. As an example, the generic cyber capability of using a targeted Trojan to plant a kill switch may breach the rule prohibiting indiscriminate weapons—or it may not. Much will depend (i) on the nature and characteristics of the chosen targeted computer system; (ii) the customers of the target system; (iii) on whether those customers are liable further to spread the malware—innocently or otherwise; (iv) on whether the kill switch when used against the intended target is designed to cause death, injury or damage; and (v) on numerous other features peculiar to the specific intended cyber operation.

Accordingly, a weapon review of such a generic capability should consider the likely applications of the cyber tool, taking into account what the tool is designed to do and how it is designed to do it. The review should discuss which potential applications, if any, would breach the weapons law rules applicable to that State and should identify whether there are restrictions on the lawful use of the cyber tool. It will then be for the legal adviser to the operational commander to consider the intended cyber operation by reference to both weapons law and targeting law norms.

It is evident from the analysis in this article that a useful focus for future research and cyber weapons development would be to enhance the ability of a cyber attacker to control and limit the effects of cyber weapons. This implies the need to be able to direct the weapon at the intended target, to limit its effects to that target and to be able to switch off the damaging operations if it ceases to operate as intended. Cyber weapons that lack any of these features will not necessarily be unlawful; however, enhancing the ability to control—possibly even to reverse—cyber effects would seem to be a future, if not a present, priority given ever increasing cyber dependence.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

International Law and Cyber Threats from Non-State Actors

Laurie R. Blank

89 INT'L L. STUD. 406 (2013)

Volume 89 2013

International Law and Cyber Threats from Non-State Actors

Laurie R. Blank[*]

I. INTRODUCTION

The so-called "virtual" world, that of the Internet, computer networks and cyberspace in general, is now very firmly part of the "real world," especially in the areas of national security and military strategy. Revolutionary advances in technology now enable both militaries and civilians to engage in cyber activity to achieve objectives, whether related to protest and revolution, crime, terrorism, espionage or military operations. At one end of the spectrum both governments and private companies face a nearly constant onslaught of cyber activity seeking to access information, undermine or damage systems, or otherwise gain a financial, political or strategic advantage of some kind. At the other end of the spectrum are acts that some commentators call "cyber war" or "cyber attacks," including the cyber operations in Georgia during the 2008 conflict between Russia and Georgia, the Stuxnet virus or the comprehensive computer network operations launched against the Estonian government in the summer of 2007. Governments and companies alike have established both formal and informal mechanisms for countering these rapidly developing threats and operations in cyberspace, including, for example, U.S. Cyber Command, China's Peo-

* Director, International Humanitarian Law Clinic, Emory University School of Law.

ple's Liberation Army General Staff Department's 3rd Department, Iranian Sun-Army and Cyber Army, Israel's Unit 8200, and the Russian Federal Security Service's 16th Directorate.

Rhetoric has matched these developments as well. We now read about a wide range of cyber "things:" cyber crime, cybersecurity, cyber espionage, cyber threats, cyber attacks, cyber war or warfare, cyber terrorism and so on. A look at news coverage of these issues in recent years demonstrates the growing focus across a range of countries, industries and disciplines, with the number of news stories mentioning either "cyber war," "cyber warfare" or "cyber attack" in 2010 or 2011 more than triple that of any previous year before 2009.[1] The number of scholarly articles, academic conferences, policy discussions and other events addressing cyber issues is further evidence of the extent of the current discourse.

Within the realm of law applicable to and governing cyber activity, a host of legal regimes are relevant, including, most notably, domestic criminal law, national security law and international law. Just as examples, the U.S. Congress has engaged in extensive debate over various forms of cybersecurity legislation[2] and international experts have devoted—and continue to devote—significant energy to examining the extent and nature of the application of international law to cyber war and related activities.[3] In addition, the nature of cyber operations, computer networks, the Internet and related components of the cyber arena mean that a veritable plethora of actors are and can be involved in cyber activities. Among these are militaries, other government agencies, private companies, terrorist groups and individuals acting on a range of different motivations, often referred to as "hacktivists." The nature of today's globalized and interconnected world combined with the extensive reliance on technology, computer systems and Internet connectivity means that non-State actors, whether individuals or groups of some kind, can have a significant impact through cyber activity.

---

1. A brief Lexis-Nexis search of major newspapers shows 944 and 965 hits for the term "cyber attack" in 2010 and 2011, respectively, compared to approximately 200 or fewer for any year before 2009. The same general pattern holds true for the terms "cyber war" and "cyber warfare." Based on the first few months of 2012, news coverage looks to be comparable to that of the previous two years.

2. *See, e.g.*, Paul Rosenzweig, *The Politics of the Cyber-Legislation Debate*, LAWFARE (Apr. 19, 2012, 11:48 AM), http://www.lawfareblog.com/2012/04/the-politics-of-the-cyber-legislation-debate/.

3. *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013).

At the same time, the complexity of cyber operations—in terms of characterizing the nature of the operations, identifying the main players and developing appropriate options in response—opens up an equally complex legal environment for analyzing the parameters of and framework for such responses. This legal environment includes the law of armed conflict (LOAC), the law governing the resort to force *(jus ad bellum)* and human rights law, along with national security law and domestic criminal law. Cyber operations can be used both in armed conflict and in the absence of armed conflict, which is, of course, part of the complex nature of the legal inquiry. A host of interesting questions arise from the use of cyber capabilities by States and non-State actors, including when cyber acts trigger the international law regime governing the use of force and/or LOAC and the nature of self-defense in response to cyber acts, in particular, against non-State actors, and the contours of a cyber battlespace, to name a few. Furthermore, both *jus ad bellum* and LOAC pose challenging questions regarding the appropriate application of the law and the parameters of the legal paradigm at issue. This article will focus on the international legal framework that governs defense against cyber threats from non-State actors, specifically LOAC and the law governing the resort to force. In doing so, it will identify both essential paradigms for understanding options for response to cyber threats from non-State actors and key challenges in those paradigms. Section II addresses *jus ad bellum* and how it applies to and provides guidance for State responses to cyber actions by non-State actors. Section III analyzes when and how LOAC applies to non-State cyber acts and examines some of the specific challenges cyber acts pose for such analysis. Finally, Section IV highlights broader crosscutting issues, such as the challenges of multiple overlapping legal paradigms and the role and power of rhetoric, in exploring how States can and do respond to cyber threats from non-State actors.

The current discourse about cyber war suggests a look back at the discourse surrounding appropriate responses to terrorist attacks and terrorist groups in the aftermath of the September 11 attacks. Questions abounded, for example, regarding whether responses to terrorists fell within a law enforcement paradigm or a war paradigm, whether the same international law that governed hostilities and law enforcement in other situations should also guide responses to terrorists, and whether terrorists were entitled to basic rights under either human rights law or LOAC. The debate and discourse about cyber war are in many ways wholly different: extensive legal analysis and debate are preceding action and few commentators or policy-

makers are proposing that cyberspace be a "law-free" arena. However, some aspects of the past decade of debate over lawful counterterrorism policy offer useful lessons for exploring the legal regime governing cyber operations, including the role of rhetoric and the need to understand the interplay between multiple overlapping legal frameworks.

As a preliminary matter, it is useful to note that cyber activities take place along an expansive continuum with information analysis and gathering at one end and hostilities at the other, roughly, and including espionage, surveillance, crime and other activities along its span. In many cases, it is likely that groups or individuals will engage in operations that fall within more than one category along that continuum, thus triggering potential application of multiple legal frameworks. Terrorist attacks pose many of the same challenges. A terrorist attack is, at a minimum, a crime, but over the past decade it has become accepted fact that terrorist attacks can also be hostilities that constitute an armed conflict. As a result, policymakers and academics have engaged in extensive debate regarding whether responses to terrorism fall within a law enforcement paradigm or a war paradigm. Although the full parameters of that debate are outside the scope of this article, the debate itself offers useful lessons in recognizing the multiple legal paradigms applicable to cyber activities and analyzing how and in what situations they apply. Throughout the analysis, therefore, this article will often refer to existing and developing considerations in responses to non-State terrorist entities, both in rhetoric and in policy and legal choices, as appropriate in examining the legal paradigms for responding to cyber threats from non-State actors.

II. THE LAW GOVERNING THE RESORT TO FORCE

In many cases, the cyber activity of non-State actors falls squarely within a broad category of cyber crime, but perhaps can also be categorized as cyber espionage. Some acts, however, pose a threat not just to private companies or industry, but in a more comprehensive way to the national security of the State. Cyber warfare thus has been defined broadly to include, among other actions, defending information and computer networks, deterring information attacks, denying an adversary's ability to defend networks and deter attacks, engaging in offensive information operations against an ad-

versary and dominating information on the battlefield.[4] The transition from domestic and cross-border law enforcement to more forceful responses depends on an analysis of how and when international law establishes a right for States to use force and in what manner. The increasing focus on cyber operations by both States and non-State actors has led to an extensive discourse on the question of when an action in the cyber realm constitutes a use of force,[5] a key preliminary question in any discussion regarding the legality of the use of force in the cyber arena. This article, which focuses specifically on responding to non-State actors in the cyber realm, will use that discourse as a backdrop, but will not delve into a discussion of what constitutes a use of force generally for the purposes of *jus ad bellum*. Rather, since there is extensive scholarship on the question of what cyber activity constitutes a use of force,[6] the instant discussion will assume the existence of a use of force and proceed to the next step in the legal analysis. Furthermore, this article will not address the legal questions surrounding when a State may attribute the acts of a non-State actor to a State for the purposes of responding to threats or attacks by using force against that State.

Jus ad bellum is the Latin term for the law governing the resort to force—that is, when a State may use force within the constraints of the United Nations Charter framework and traditional legal principles. The modern *jus ad bellum* has its origins in the 1919 Covenant of the League of Nations, the 1928 Kellogg-Briand Pact and the United Nations Charter.[7] In particular, Article 2(4) of the United Nations Charter prohibits the use of force by one State against another: "All members shall refrain in their in-

4. *See* STEPHEN HILDRETH, CONGRESSIONAL RESEARCH SERVICE, RL30735, CYBERWARFARE 16–17 (2001), *available at* http://www.fas.org/irp/crs/RL30735.pdf.

5. *See* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885 (1999); Eric Talbot Jensen, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense,* 38 STANFORD JOURNAL OF INTERNATIONAL LAW 207 (2002); Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421 (2011); Eric Talbot Jensen, *President Obama and the Changing Cyber Paradigm*, 37 WILLIAM MITCHELL LAW REVIEW 5049 (2011); Sean Watts, *Low-Intensity Computer Network Attack and Self-Defense*, *in* INTERNATIONAL LAW AND THE CHANGING CHARACTER OF WAR 59 (Raul A. "Pete" Pedrozo & Daria P. Wollschlaeger eds., 2011) (Vol. 87, U.S. Naval War College International Law Studies); Matthew Hoisington, *Note: Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*, 32 BOSTON COLLEGE JOURNAL OF INTERNATIONAL LAW 439 (2009).

6. *See, e.g.*, Schmitt, *supra* note 5; Jensen, *Computer Attacks on Critical National Infrastructure*, *supra* note 5; Waxman, *supra* note 5.

7. MALCOLM N. SHAW, INTERNATIONAL LAW 780–81 (4th ed. 1997).

ternational relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations."[8] This provision, by placing severe restrictions and prohibitions on the use of force, is in many ways the foundation of the UN's goal of "sav[ing] succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind."[9]

The Charter provides for three exceptions to the prohibition on the use of force, each of which is relevant to cyber operations in response to a threat from a non-State actor. First, a State may use force with the consent of the territorial State, such as when a State battling a rebel group requests assistance from one or more other States. In such cases, the territorial State can only consent to such assistance and uses of force in which it could legally engage—no State can consent to actions by another State that would violate international law if undertaken by the requesting State. To the extent that a State engages in cyber operations that rise to the level of a use of force in such a context, it would thus need to ensure that such use of force remained within the parameters of actions the territorial State could lawfully undertake. Second, a State can use force as part of a multinational operation authorized by the Security Council under Chapter VII, as provided in Article 42.

Third, a State may use force in accordance with the inherent right of self-defense under Article 51 in response to an armed attack. This provision builds on and establishes the basic framework of the *jus ad bellum*, stating: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security."[10] It is in this context that most issues and considerations regarding defense against cyber threats from non-State actors will arise. As a result, it is helpful to first set forth the basic contours of international law with regard to the use of force in self-defense.

The classic formulation of the parameters of self-defense stems from the *Caroline* incident. British troops crossed the Niagara River to the American side and attacked the steamer *Caroline*, which had been running arms and materiel to insurgents on the Canadian side. The British justified the

8. U.N. Charter art. 2, para. 4.
9. *Id.*, pmbl.
10. *Id.*, art. 51.

attack, in which they set fire to the *Caroline* and killed one American, on the grounds that their troops had acted in self-defense. In a letter to his British counterpart, Lord Ashburton, U.S. Secretary of State Daniel Webster declared that the use of force in self-defense should be limited to "cases in which the 'necessity of that self-defence is instant, overwhelming, and leaving no choice of means, and no moment for deliberation.'"[11] Furthermore, the force used must not be "unreasonable or excessive; since the act, justified by the necessity of self-defence, must be limited by that necessity, and kept clearly within it."[12] Much of the extensive literature analyzing the right of self-defense, and, in particular, the parameters of the right of self-defense in response to terrorist attacks,[13] offers a useful foundation for the instant analysis.

A. The Right to Respond to Cyber Threats from Non-State Actors

A State that faces cyber threats from or attacks by non-State actors can respond as long as the response is lawful within the context of the *jus ad bellum*. Any lawful use of force in self-defense depends initially on the existence of an armed attack. Note that an armed attack is more severe and significant than a use of force, meaning that a State can be the victim of a

---

11. Letter from Daniel Webster, U.S. Secretary of State, to Lord Ashburton, Special British Minister (Aug. 6, 1842), *in* 2 JOHN BASSETT MOORE, A DIGEST OF INTERNATIONAL LAW § 217 at 412 (1906).

12. Letter from Daniel Webster, U.S. Secretary of State, to Henry Fox, British Minister in Washington (Apr. 24, 1841), *in* 29 BRITISH & FOREIGN STATE PAPERS 1840–1841, at 1138 (1857).

13. *See, e.g.*, YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 175–82 (2d ed. 1994) (discussing the concept and right of self-defense); David Kretzmer, *Targeted Killing of Suspected Terrorists: Extra-Judicial Executions or Legitimate Means of Defence?*, 16 EUROPEAN JOURNAL OF INTERNATIONAL LAW 171, 173 (2005) (noting that some States argue that targeted killings are within the "state's inherent right to self-defence"); Craig Martin, *Going Medieval: Targeted Killing, Self-Defence, and the* Jus ad Bellum *Regime*, *in* TARGETED KILLINGS: LAW & MORALITY IN AN ASYMMETRICAL WORLD 223 (Claire Finkelstein, Jens David Ohlin & Andrew Altman eds., 2012) (discussing the validity of a self-defense claim regarding targeted killing of suspected terrorists); Jordan J. Paust, *Self-Defense Targetings of Non-State Actors and Permissibility of U.S. Use of Drones in Pakistan*, 19 JOURNAL OF TRANSNATIONAL LAW & POLICY 237 (2010) (arguing that self-defense is permissible against non-State actors who commit armed attacks and that actions of self-defense can be made in another State without that State's consent); Michael N. Schmitt, *Responding to Transnational Terrorism Under the* Jus ad Bellum*: A Normative Framework*, 56 NAVAL LAW REVIEW 1 (2008) (noting that the "United States claim[ed] self-defense as a right in forcefully countering terrorism").

use of force without being the victim of an armed attack that triggers the right of self-defense.[14] In assessing whether a particular hostile action directed at a State rises to the level of an armed attack, the International Court of Justice (ICJ) looks at the scale and effects of the act.[15] For example, if a State deploys its regular armed forces across a border, that will generally be considered an armed attack, as will a State's sending irregular militias or other armed groups to accomplish the same purposes. In contrast, providing weapons or other assistance to rebels or other armed groups across State borders will not reach the threshold of an armed attack.

Directly related to the analysis of self-defense against cyber threats or attacks by non-State actors, a key *jus ad bellum* question is whether only States can launch an armed attack. Nothing in Article 51 specifies that the right of self-defense is only available in response to a threat or use of force by another State. Nonetheless, the precise contours of what type of actor can trigger the right of self-defense remains controversial. Some argue that only States can be the source of an armed attack—or imminent threat of an armed attack—that can justify the use of force in self-defense.[16] The ICJ has continued to limit the right in this manner in a series of cases.[17] However, State practice in the aftermath of the 9/11 attacks provides firm support for the existence of a right of self-defense against non-State actors, even if unrelated to any State.[18] Indeed, the *Caroline* incident, which forms

14. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 191 (June 27) [hereinafter *Military and Paramilitary Activities*]. *See also* Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict*, *in* COMMITTEE ON DETERRING CYBERATTACKS, NATIONAL RESEARCH COUNCIL, PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS: INFORMING STRATEGIES AND DEVELOPING OPTIONS FOR U.S. POLICY 163 (2010), *available at* http://books.nap.edu/openbook.php?record_id=12997&page=R1.

15. *Military and Paramilitary Activities*, *supra* note 14.

16. *See, e.g.*, Antonio Cassese, *The International Community's "Legal" Response to Terrorism*, 38 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 589, 597 (1989); Eric Myjer & Nigel White, *The Twin Towers Attack: An Unlimited Right to Self-Defense*, 7 JOURNAL OF CONFLICT AND SECURITY LAW 5, 7 (2002) ("Self-defense, traditionally speaking, applies to an armed response to an attack by a state.").

17. *See, e.g.*, *Military and Paramilitary Activities*, *supra* note 14; Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161 (Nov. 6); Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168 (Dec. 19); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, 215 (July 9).

18. *See, e.g.*, DINSTEIN, *supra* note 13, at 214; Christopher Greenwood, *International Law and the Preemptive Use of Force: Afghanistan, al Qaeda, and Iraq*, 4 SAN DIEGO INTERNATIONAL LAW JOURNAL 7, 17 (2003) (discussing the effects of attacks made by non-State

the historical foundation of the right to self-defense, involved an armed attack by non-State actors. UN Security Council Resolution 1368, for example, recognized the inherent right of self-defense against the September 11 attacks and "[u]nequivocally condemn[ed] in the strongest terms the horrifying terrorist attacks which took place on 11 September 2001 in New York, Washington, D.C. and Pennsylvania and *regard[ed]* such acts, like any act of international terrorism, as a threat to international peace and security."[19] Similarly, the North Atlantic Council issued a statement activating the collective self-defense provision in Article 5 of the North Atlantic Treaty, as did the Organization of American States regarding its constituent treaty.[20] Several other States have asserted the same right, including Turkey, Israel, Colombia and Russia.[21] Over the past decade, the challenge of responding to transnational terrorism has helped drive State practice and debate regarding the lawfulness of self-defense in response to armed attacks by non-State actors.

Although the analysis may seem relatively straightforward in the con-

---

actors); Sean D. Murphy, *The International Legality of US Military Cross-Border Operations from Afghanistan into Pakistan*, *in* THE WAR IN AFGHANISTAN: A LEGAL ANALYSIS 109, 126 (Michael N. Schmitt ed., 2009) (Vol. 85, U.S. Naval War College International Law Studies) ("While this area of the law remains somewhat uncertain, the dominant trend in contemporary interstate relations seems to favor the view that States accept or at least tolerate acts of self-defense against a non-State actor."); Raphaël Van Steenberghe, *Self-Defence in Response to Attacks by Non-state Actors in the Light of Recent State Practice: A Step Forward?*, 23 LEIDEN JOURNAL OF INTERNATIONAL LAW 183, 184 (2010) (concluding that recent State practice suggests that attacks committed by non-State actors alone constitute armed attacks under Article 51).

19. S.C. Res. 1368, ¶ 1, U.N. Doc. S/RES/1368 (Sept. 12, 2001) (emphasis added).

20. North Atlantic Treaty art. 5, Apr. 4, 1949, 63 Stat. 2241, 2244, 34 U.N.T.S. 243, 246; Press Release, North Atlantic Treaty Organization, Statement by the North Atlantic Council (Sept. 12, 2001), *available at* http://www.nato.int/docu/pr/2001/p01-124e.htm; Inter-American Treaty of Reciprocal Assistance art. 3.1, Sept. 2, 1947, 62 Stat. 1681, 1700, 21 U.N.T.S. 77, 93; Terrorist Threat to the Americas, Res. 1, Twenty-Fourth Meeting of Consultation of Ministers of Foreign Affairs Acting as Organ of Consultation in Application of the Inter-American Treaty of Reciprocal Assistance, OEA/Ser.F/II.24, RC.24/RES.1/01 (Sept. 21, 2001). Similarly, Australia activated the collective self-defense provision of the ANZUS Pact. Security Treaty Between Australia, New Zealand and the United States of America art. IV, Sept. 1, 1951, 3 U.S.T. 3420, 3423, 131 U.N.T.S. 83, 86; Brendan Pearson, *PM Commits to Mutual Defence,* AUSTRALIAN FINANCIAL REVIEW, Sept. 15, 2001, at 9.

21. For an extensive treatment and discussion of the use of force in self-defense and State practice, see Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VIRGINIA JOURNAL OF INTERNATIONAL LAW 483 (2012).

text of military units, armed bands and kinetic force, in the cyber realm, identifying and analyzing an armed attack are significantly more challenging. The most common method of analysis with regard to whether cyber actions rise to the level of an armed attack is an effects-based analysis. At present, there is a general consensus that "any use of force that injures or kills persons or damages or destroys property" constitutes an armed attack, including in the cyber arena.[22] Others point to the target of a cyber operation, arguing that any cyber action against critical national infrastructure should qualify as an armed attack,[23] or, alternatively, to an "instrument-based" approach, according to which a cyber operation constitutes an armed attack if "the damage caused by a cyber attack could previously have been achieved only by a kinetic attack."[24] In contrast, economic damage, political embarrassment or coercion, a disruption of communications, and the distribution of propaganda through cyber means do not rise to the level of an armed attack. The *Tallinn Manual on International Law Applicable to Cyber Warfare* explains that cyber intelligence gathering and theft do not constitute an armed attack, nor would "cyber operations that involve brief or periodic interruption of non-essential cyber services."[25]

Responding to cyber threats or attacks by non-State actors within this paradigm poses several challenging questions beyond the characterization of an armed attack or the continued—although waning—uncertainty regarding whether non-State actors could alone launch an armed attack that triggers the right of self-defense. The first such question stems from one of the fundamental challenges of cyber activity: attribution. Identifying the source of an attack is a uniquely complex and difficult act in the cyber arena; these challenges add an additional layer of legal uncertainty in analyzing a State's right to respond in self-defense. Although general consensus exists, particularly in the discourse on cyber warfare, that attacks by non-State actors (those not related or attributable to a State) can trigger the right of self-defense,[26] what about a lone wolf actor? Or a loosely knit group of hacktivists? The traditional notion of a non-State actor launching an armed

22. TALLINN MANUAL, *supra* note 3, at 54.

23. Jensen, *Computer Attacks on Critical National Infrastructure*, *supra* note 5 at 221–26.

24. David E. Graham, *Cyber Threats and the Law of War*, 4 JOURNAL OF NATIONAL SECURITY LAW AND POLICY 87, 91 (2010) (citing Yoram Dinstein, *Computer Network Attacks and Self-Defense*, *in* COMPUTER NETWORK ATTACK AND INTERNATIONAL LAW 99, 103–5 (Michael N. Schmitt & Brian T. O'Donnell eds., 2002) (Vol. 76, U.S. Naval War College International Law Studies)).

25. TALLINN MANUAL, *supra* note 3, at 55.

26. *Id.* at 57.

attack on a State conjures images of rebel groups or guerrilla fighters—some type of organized entity with a name, a structure and, likely, some method of directing operations.[27] Cyber warfare in particular raises the specter of a solo actor, or perhaps a small handful of actors, who can pose a devastating threat to a State through a cyber attack. In the absence of evidence linking an individual or individuals to a State or a larger, more organized entity, it is unclear whether such an attack falls within the right of self-defense or would remain, in essence, in the criminal arena. Counterterrorism does offer some useful analogies in this respect, particularly in the current environment of attacks conducted against terrorist operatives in far-flung regions of Pakistan and Yemen. The United States relies on self-defense as one primary justification for the use of force against terrorist operatives;[28] however, it always presents the target as a member of al Qaeda or affiliated terrorist groups, thus not offering any firm evidence of the use of force against a solo actor. Nonetheless, it is not inconceivable—although it is perhaps highly unlikely—that the United States or other State actor might argue that force is the only recourse to repel or deter an armed attack by a lone-wolf actor in a particular circumstance.

Attribution poses a second challenge as well. In using force in self-defense against a non-State actor, the State using force will be doing so in the territory of another State, one that did not launch the original attack and does not bear direct responsibility for the attack. The responding State must, therefore, act either with the consent of the territorial State or on the grounds that the territorial State is unwilling or unable to take action to remove the threat posed by the non-State actor and prevent future attacks.[29] The notions of unwilling or unable are not necessarily fully defined in the realm of kinetic attacks, and attribution challenges make them much harder to apply in the cyber arena. At the preliminary level, the inherently obscure nature of cyber activities can make it difficult to tell the specific location from which the attack emanated—including which State—thus undermining the ability to use the unwilling or unable formulation as a foundation

27. *See infra* pp. 428 - 429 for a more detailed discussion of the notion of an organized armed group within the cyber context.

28. Harold Hongju Koh, Legal Adviser, U.S. Department of State, *Keynote Address at the Annual Meeting of the American Society of International Law: The Obama Administration and International Law* (Mar. 25, 2010), http://www.state.gov/s/l/releases/remarks/139119.htm. *See also* Laurie R. Blank, *Targeted Strikes: The Consequences of Blurring the Armed Conflict and Self-Defense Justifications*, 38 WILLIAM MITCHELL LAW REVIEW 1655 (2012).

29. *See generally* Deeks, *supra* note 21 (examining in depth the historical and legal foundations of the "unwilling or unable" test).

for responsive action. In this respect, cyber poses perhaps unique challenges because of the ability to dissemble and present an attack as coming from one or more different States or locations, or simply because an attack passes through or can be traced back to multiple—even over a hundred—States.[30] For this reason, the victim State must tread carefully and seek as much clarity regarding the source of the attack as possible to avoid launching a self-defense response in the wrong direction. This challenge is particularly acute with regard to responding to attacks by non-State actors unaffiliated with a State because there may well be fewer accountability trails to follow or venues for attributing responsibility.

Finally, the cyber arena is particularly relevant to the question of whether a series of lower-level attacks or incidents can combine together to rise to the level of an armed attack that triggers the right of self-defense. Some argue that "gaps in [*jus ad bellum*'s] response structure will prove highly susceptible to low-intensity cyber attacks, leaving victim States to choose between enduring damaging intrusions and disruptions or undertaking arguably unlawful unilateral responses."[31] In effect, because of the distinction between a mere use of force, which does not trigger the right of self-defense, and the more significant armed attack, which does trigger that right, there is fertile ground for extensive and disruptive cyber activity that does not necessarily provide the victim State with significant opportunities for a useful response. Here, attribution plays a key role again. To the extent that a State can determine that a series of low-level cyber incidents originate from the same source—the same non-State actors or entity—then there is a strong argument to be made that, taken together, the incidents constitute an armed attack to which the State can lawfully respond in self-defense.[32]

B. The Nature of Responses to Cyber Attacks by Non-State Actors

If a State has been the victim of a cyber event that meets the threshold for an armed attack, it can, under the *jus ad bellum*, respond with force in self-

30. For example, the distributed denial of service attacks on Estonia in 2007 were ultimately traced back to over 178 States. *See* Jason Healey, *Beyond Attribution: Seeking National Responsibility for Cyber Attacks*, ATLANTIC COUNCIL (Jan. 2012), https://www.fbiic.gov/public/2012/mar/National_Responsibility_for_CyberAttacks,_2012.pdf.

31. Sean Watts, *supra* note 5, at 60–61.

32. TALLINN MANUAL, *supra* note 3, at 55 (noting also that this approach is called the "pin-prick theory" or the "accumulation of effects theory").

defense. In so doing, the State must comport with the requirements of necessity, proportionality and immediacy.[33] As a first step, the law does not constrain a State responding to a cyber attack to use only cyber force in response. The victim State can use kinetic force in self-defense as a response to a cyber attack if that use of kinetic force comports with the requirements of necessity and proportionality.

The requirement of necessity addresses whether there are adequate non-forceful options to deter or defeat the attack, such as diplomatic avenues, defensive measures to halt any further attacks or reparations for injuries caused. Necessity includes not only action taken to halt and defeat an initial attack, but broader action to eliminate a continuing threat. More specifically, in the cyber realm, necessity requires an understanding of the ability to achieve the desired end to the threat or attack using a range of options in both the cyber and non-cyber arenas. Thus, if an armed attack by a non-State actor exposes and takes advantage of a particular vulnerability in a State's cyber defenses that can then be repaired to deny further cyber incursions, such bolstering of defenses might be a sufficient non-forceful alternative, making the use of force unlawful. In the case of attacks by non-State actors, States seeking to act in self-defense must first explore whether the territorial State can take action to stop the non-State actors from launching further attacks, including, potentially, detention of those responsible, as part of determining whether there are any non-forceful alternatives available. As noted above, the attribution challenges inherent in cyber activity can make this aspect of the *jus ad bellum* difficult to analyze.

The requirement of proportionality measures the extent of the use of force against the overall military goals, such as fending off an attack or subordinating the enemy. Rather than addressing whether force may be used at all—which is the main focus of the necessity requirement—proportionality looks at how much force may be used. In doing so, proportionality focuses not on some measure of symmetry between the original *attack* and the use of force in response, but on whether the measure of counterforce used is proportionate to the needs and goals of *repelling* or *deterring* the original attack.[34] The force used may indeed be significantly

33. These obligations form part of customary international law and have been reaffirmed numerous times by the International Court of Justice. *See, e.g.*, *Military and Paramilitary Activities*, *supra* note 14, ¶¶ 176, 194; Oil Platforms, *supra* note 17, ¶¶ 43, 73–74, 76; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 41 (July 8) [hereinafter *Nuclear Weapons*].

34. YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 237 (4th ed. 2005).

greater than that used in the attack that triggered the right to self-defense—what matters is the result sought, not the equivalence between attack and response. For this reason, there could be circumstances in which kinetic force is an appropriate—that is, proportionate—response to a cyber attack, even though it appears, at first blush, to be force of an entirely different nature from that used in the initial attack.[35] This can be especially true in examining a State's response to a cyber attack by a non-State actor. The non-State actor simply may not be vulnerable to cyber force in the same manner as a State with its critical infrastructure and national security considerations. The use of cyber force against that non-State actor may not have the desired effect of repelling the attack or deterring the non-State actor from continuing the attack or launching additional attacks because it cannot cause sufficient consequences in that scenario. Kinetic force is, under these circumstances, more likely to have that effect and be able to achieve the goal of ending the attack(s).

The final requirement for the lawful use of force in self-defense is immediacy. In the case of a response to an ongoing attack, immediacy is not relevant—necessity and proportionality will dominate the analysis of whether the use of force is appropriate. Immediacy considerations arise when a State uses force in self-defense in advance of an attack or long after an attack is over. In the latter case, a forceful response long after an attack will no longer serve defensive purposes, but will be retaliatory, and therefore unlawful. The first scenario is often termed anticipatory self-defense—the use of force to prevent an imminent attack and the death and damage it will cause. As in other components of the *jus ad bellum* analysis, cyber activity poses some unique considerations with regard to the requirement of immediacy. In many cases, the instantaneous nature of cyber operations means that the immediacy requirement is effectively inconsequential, because the moment the attack is initiated, it is also fulfilled and the damage is caused. Alternatively, however, some cyber operations, such as a logic bomb—a piece of code deliberately inserted into a software system that triggers destructive or malicious functions upon certain specified conditions—have a lag time that can make the immediacy analysis more challenging, especially in conjunction with the necessity requirement. Although

35. The United States has clearly stated that it reserves the right to use both cyber and kinetic force, as needed, in response to cyber attacks or imminent cyber attacks. *See* U.S. Department of Defense, Cyberspace Policy Report 4 (2011), *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf.

the armed attack may occur at the moment when the logic bomb is inserted into the software, fulfilling the immediacy requirement, to the extent that a State has non-forceful options for "defusing" the logic bomb before it is actually triggered, the lag time would mean that necessity is not present if such alternatives exist.

III. THE LAW OF ARMED CONFLICT

A second category or legal paradigm that applies—in different circumstances—to a State's response to cyber threats or attacks by non-State actors is the law of armed conflict. LOAC, also known as the law of war and international humanitarian law, governs the conduct of both States and individuals during armed conflict. It seeks to minimize suffering in war by protecting persons not participating in hostilities and by restricting the means and methods of warfare.[36] LOAC applies during all situations of armed conflict, with the full panoply of the Geneva Conventions and customary law applicable in international armed conflict and a more limited body of treaty and customary law applicable during non-international armed conflict. The lawfulness of targeting individuals and objects during armed conflict is determined by the principles of distinction, proportionality and precautions. With regard to the cyber arena, questions regarding responses to non-State actors fall into two primary areas: (1) the situation in which the State seeks to respond to the non-State actor in an armed conflict such that LOAC does apply; and (2) the status or nature of the non-State actors for the purposes of analyzing whether and how the State can

36. *See* International Committee of the Red Cross, *What Is International Humanitarian Law?*, ICRC (July 31, 2004), http://www.icrc.org/eng/resources/documents/legal-fact-sheet/humanitarian-law-factsheet.htm. The law of armed conflict is codified primarily in the four Geneva Conventions of August 12, 1949, and their Additional Protocols. Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 [hereinafter GC I]; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 [hereinafter GC II]; Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III]; Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC IV]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609.

target and/or detain them in the course of that conflict.

A. Does the State vs. Non-State Activity Constitute an Armed Conflict?

LOAC applies only during an armed conflict; thus determining whether the violence between the State and the non-State actor rises to the level of an armed conflict is the essential first analytical step in understanding if the State may respond to cyber threats posed by non-State actors within the paradigm of armed conflict. The 1949 Geneva Conventions endeavor to address all instances of armed conflict[37] and set forth two primary categories of armed conflict that trigger the application of LOAC: international armed conflict and non-international armed conflict. Common Article 2 of the 1949 Geneva Conventions states that the Conventions "shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them."[38] Common Article 3 of the 1949 Geneva Conventions sets forth minimum provisions applicable "in the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties."[39] Notably, the Geneva Conventions adopted the term "armed conflict" specifically to avoid the technical legal and political pitfalls of the term "war."[40] As such, determination of the existence of an armed conflict does not turn on a formal declaration of war—or even on how the participants characterize the hostilities—but rather on the facts of a given situation.[41]

---

37. COMMENTARY ON GENEVA CONVENTION IV RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR 26 (Oscar M. Uhler & Henri Coursier eds., 1958) [hereinafter GC IV COMMENTARY] ("Born on the battlefield, the Red Cross called into being the First Geneva Convention to protect wounded or sick military personnel. Extending its solicitude little by little over other categories of war victims, in logical application of its fundamental principle, it pointed the way, first to the revision of the original convention, and then to the extension of legal protection in turn to prisoners of war and civilians. The same logical process could not fail to lead to the idea of applying the principle in *all* cases of armed conflicts, including those of an internal character.").

38. GCI, GC II, GC III, GC IV art.2, *supra* note 36 [hereinafter Common Article 2].

39. *Id.*, art. 3.

40. GC IV COMMENTARY, *supra* note 37, at 17–25.

41. Common Article 2 of the 1949 Geneva Conventions applies to "all cases of declared war or of any other armed conflict . . . between two or more [States], even if the state of war is not recognized by one of them." Common Article 2, *supra* note 38. *See, e.g.*, Anthony Cullen, *Key Developments Affecting the Scope of Internal Armed Conflict in International*

The International Criminal Tribunal for the former Yugoslavia (ICTY) set forth the modern definition of armed conflict in *Prosecutor v. Tadić*, stating that an armed conflict exists whenever "there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State."[42] This definition describes both international armed conflict (armed force between States) and non-international armed conflict (protracted armed violence between governments and organized armed groups). In this subsection, the discussion will focus on the legal issues in identifying a non-international armed conflict between a State and non-State actors within the cyber arena. Of course, a State involved in an international armed conflict with another State may well face cyber threats from a non-State actor also participating in the conflict, perhaps acting in coordination with the opposing State, but the questions surrounding how the nature of that non-State actor impacts the identification of an armed conflict and the actual triggering of LOAC would not arise in the same way. As jurisprudence stemming from this definition has developed over the past two decades with regard to non-international armed conflict, two considerations have dominated the discourse, particularly in the decisions of the ICTY and other international tribunals—the intensity of the fighting and the organization of the parties.[43]

Intensity requires an analysis of the seriousness of the fighting in order to determine whether it has passed from riots and other random acts of violence to engagements more akin to regularized military action. There is little doubt that a cyber-based conflict could, at some point, reach a sufficient level of intensity to satisfy this threshold; however, the evidence or

---

Humanitarian Law, 183 MILITARY LAW REVIEW 66, 85 (2005) ("[I]t is worth emphasizing that recognition of the existence of armed conflict is not a matter of state discretion.").

42. Prosecutor v. Tadić, Case No. IT-94-1, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the former Yugoslavia Oct. 2, 1995) [hereinafter *Prosecutor v. Tadić* (Decision on Interlocutory Appeal)].

43. Prosecutor v. Tadić, Case No. IT-94-1-T, Judgment, ¶ 562 (Int'l Crim. Trib. for the former Yugoslavia May 7, 1997) [hereinafter *Prosecutor v. Tadić* (Judgment)]; Prosecutor v. Limaj, Case No. IT-03-66-T, Judgment, ¶ 84 (Int'l Crim. Trib. for the former Yugoslavia Nov. 30, 2005); Prosecutor v. Boskoski & Tarculovski, Case No. IT-04-82-T, Judgment, ¶ 175 (Int'l Crim. Trib. for the former Yugoslavia July 10, 2008). For a counterargument to the increasingly formalized application of these two elements or factors, see Laurie R Blank and Geoffrey S. Corn, *Losing the Forest for the Trees: Syria, Law and the Pragmatics of Conflict Recognition*, 46 VANDERBILT JOURNAL OF TRANSNATIONAL LAW (forthcoming 2013).

analysis of such intensity could differ from the factual information used in a kinetic scenario. Traditionally, analyzing intensity has encompassed a range of specific factors regarding the actual hostilities. For example, the ICTY has considered factors such as the number, duration and intensity of individual confrontations; the types of weapons and other military equipment used; the number of persons and types of forces engaged in the fighting; the geographic and temporal distribution of clashes; the territory that has been captured and held; the number of casualties; the extent of material destruction; and the number of civilians fleeing combat zones.[44] The ICTY has also declared that the involvement of the UN Security Council may reflect the intensity of a conflict.[45] The collective nature of the fighting, the State's resort to use of its armed forces, the duration of the conflict, and the frequency of the acts of violence and military operations are all additional factors to take into account as well. Most or all of these considerations are highly relevant in the cyber context as well (with the exception, perhaps, of the capture of territory), but the analysis will rely overwhelmingly on the effects of attacks rather than the types of operations, the engagement of forces or the number of persons involved, because those categories of information are extremely difficult to assess in the cyber arena.

In the scenario of a potential conflict between a State and non-State actors using cyber attacks as the main form of attack, the second factor of organization is of particular interest. Various international tribunals and other courts have looked to a non-State actor's level of organization as one way to distinguish armed conflict from unorganized violence and riots. Rigid adherence to specific measures or types of organization have the potential to undermine the effectiveness of LOAC by hindering its application to situations that otherwise seem to obviously fall within the notion of an armed conflict.[46] Nonetheless, whether one takes a more formalized approach to the definition of armed conflict, relying heavily on the intensity/organization factors, or a more totality-of-the-circumstances approach, some notion of an opposing party fighting against the State is essential to characterizing a situation as an armed conflict for the application of LOAC. Here the cyber arena poses potentially unique challenges, especially in the

44. Prosecutor v. Haradinaj, Case No. IT-04-84-T, Judgment, ¶ 49 (Int'l Crim. Trib. for the former Yugoslavia Apr. 3, 2008); *Prosecutor v. Limaj*, *supra* note 43, ¶¶ 135–43; *Prosecutor v. Tadić* (Judgment), *supra* note 43, ¶¶ 564–65.

45. *Prosecutor v. Haradinaj*, *supra* note 44, ¶ 49.

46. *See* Blank and Corn, *supra* note 43.

context of non-State actors launching attacks on the State.

Factors traditionally considered as important in determining whether a group is sufficiently organized to be a party to an armed conflict include a hierarchical structure, territorial control and administration, the ability to recruit and train combatants, the ability to launch operations using military tactics and the ability to enter peace or ceasefire agreements.[47] The International Committee of the Red Cross (ICRC) has also highlighted the non-State actor's authority to launch attacks bringing together different units and the existence or promulgation of internal rules.[48] To the extent that a non-State armed group is engaged in a struggle against government forces in which cyber operations form only one tool in that struggle, the analysis will be similar to that in other situations, such as those highlighted in the ICTY's jurisprudence in which it, for example, examined the nature of the Kosovo Liberation Army in determining whether it constituted an organized armed group such that the violence in Kosovo was an armed conflict. The more interesting question and the one directly relevant to the instant analysis, however, is how to determine the existence of a non-international armed conflict when the non-State actors engage with the government solely in the cyber realm. Can a seemingly "virtual conflict" be an armed conflict that triggers LOAC?

At one end of the spectrum would be a group that is organized with some type of command structure, a decision making and operational planning process, and the ability to launch operations. In essence, the type of weapon used—cyber—would be the main distinction between this type of group and an organized armed group using kinetic force and there would be little question that such a group is sufficiently organized to meet the criterion of organization to be a party to an armed conflict. Much more likely, however, is that cyber attacks by non-State actors against a government would be carried out by independent actors, disparate actors sharing similar goals or even loosely affiliated groups of hackers or other actors. "Autonomous actors who are simply all targeting a State, perhaps in response to a broad call to do so from one or more sources," but without any formal di-

47. *See Prosecutor v. Limaj*, *supra* note 43, ¶¶ 95–109; Prosecutor v. Lukić, Case No. IT-98-32/1-T, Judgment, ¶ 884 (Int'l Crim. Trib. for the former Yugoslavia July 20, 2009); *Prosecutor v. Haradinaj*, *supra* note 44, ¶ 60.

48. Sylvain Vité, *Typology of Armed Conflicts in International Law: Legal Concepts and Actual Situations*, 91 INTERNATIONAL REVIEW OF THE RED CROSS 77 (2009).

rection or structure, "cannot be deemed to be organized."[49] As the *Commentary* to the Additional Protocols explains, "individuals operating in isolation" generally do not fit within the understanding of "organized."[50]

The nature of the virtual world, in which members of groups—even ones with a high degree of organization and shared purpose—have no face-to-face contact or connection, compounds the challenges of identifying sufficient organization to meet the definition of armed conflict. For example, during the conflict between Georgia and Russia in the summer of 2008, numerous cyber attacks were launched against Georgia. Most of these attacks were initiated using information from a website that provided cyber tools and lists of Georgian government websites and cyber targets. The attacks were not coordinated with regard to timing, target and effect, or in any other aspect. Based on existing analyses of the *Tadić* definition of armed conflict and the requisite components of the factor of organization, something more than this type of merely collective action would be needed in the solely cyber realm. It has been argued that the determination of whether a group acting for a shared purpose "meets the organization criterion should depend on such context-specific factors as the existence of a formal or informal leadership entity directing the group's activities in a general sense, identifying potential targets and maintaining an inventory of effective hacker tools."[51]

The scenario of a cyber-only engagement between non-State actors and a State that is of sufficient intensity to merit consideration as an armed conflict may seem far-fetched at this point, but it is possible and if it were to occur, it would raise questions as to whether LOAC applies. Just as the scattered nature of the opposition to government forces in a kinetic environment could forestall the recognition of an armed conflict—as the international community argued for many months with regard to the conflict in Syria[52]—such arguments would have significantly greater force in a cyber-

49. Michael N. Schmitt, *Cyber Operations and the* Jus in Bello: *Key Issues*, 41 ISRAEL YEARBOOK ON HUMAN RIGHTS 113, 124–25 (2011).

50. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 1672 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987).

51. Schmitt, *supra* note 49, at 125. Although Schmitt's analysis focuses on the identification of an organized armed group for the purposes of distinguishing members of that group from civilians in the context of a direct participation in hostilities analysis, it is equally useful in the present context of analyzing the extent of a group's organization for the purposes of finding an armed conflict that triggers the application of LOAC.

52. *See* Blank and Corn, *supra* note 43.

only engagement. It is nonetheless important to understand how the law delineates between non-conflict and armed conflict, precisely because the parameters of the government response to the non-State actors engaged in cyber operations change dramatically between the law of peacetime and the law of wartime, as the following subsection details.

B. Responding to Non-State Actors in the Course of Armed Conflict

Within the context of an armed conflict—whether mixed kinetic and cyber or perhaps solely cyber, as in the less likely scenario alluded to above—the essential issues will be identifying who or what can be targeted and who can be detained. Even more than in "normal" or kinetic conflict, in the cyber arena, intelligence information is critically important, particularly because of the heightened challenges of attribution in the cyber context. Indeed, anonymity is one of the greatest advantages that cyber warfare offers to both States and non-State actors. With regard to targeting, attribution (for both persons and objects) plays a central role in the identification of targets—mandated by the principle of distinction—but also in operationalizing the obligations of proportionality and precautions. Moreover, each of these three fundamental principles has an even more acute protective role to play in a non-international armed conflict, where the lines between fighter and civilian are often extremely blurred.

1. Identifying and Classifying Non-State Actors in Cyber Conflict

The principle of distinction, one of the "cardinal principles" of LOAC,[53] requires that any party to a conflict distinguish between those who are fighting and those who are not and direct attacks solely at the former. Similarly, parties must distinguish between civilian objects and military objects and target only the latter. Article 48 of Additional Protocol I sets forth the basic rule: "[I]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their op-

53. *Nuclear Weapons*, *supra* note 33, ¶ 78 (Higgins, J., dissenting on unrelated grounds) (declaring that distinction and the prohibition on unnecessary suffering are the two cardinal principles of international humanitarian law).

erations only against military objectives.[54]

Distinction lies at the core of LOAC's seminal goal of protecting innocent civilians and persons who are *hors de combat*. The obligation to distinguish is part of the customary international law of both international and non-international armed conflicts, as the ICTY held in the *Tadić* case.[55] The purpose of distinction—to protect civilians—is emphasized in Article 51 of Additional Protocol I, which states that "[t]he civilian population as such, as well as individual civilians, shall not be the object of attack."[56] Furthermore, Article 85 of Protocol I declares that nearly all violations of distinction constitute grave breaches of the Protocol.[57] The Rome Statute similarly criminalizes attacks on civilians and indiscriminate attacks.[58]

Distinction requires identification of lawful targets as a prerequisite to the use of force in armed conflict. A lawful attack must be directed at a legitimate target—a combatant, member of an organized armed group, civilian directly participating in hostilities or military objective. In international armed conflicts, all members of the State's regular armed forces are combatants and can be identified by the uniform they wear, among other characteristics. Other persons falling within the category of combatant include members of volunteer militias who meet four requirements: wearing a distinctive emblem, carrying arms openly, operating under responsible com-

---

54. AP I, *supra* note 36, art. 48. Article 48 is considered customary international law. *See* 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 3–8 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005) [hereinafter CIHL].

55. *Prosecutor v. Tadić* (Decision on Interlocutory Appeal), *supra* note 43, ¶ 110 ("Bearing in mind the need for measures to ensure the better protection of human rights in armed conflicts of all types, [the General Assembly] Affirms the following basic principles for the protection of civilian populations in armed conflicts, without prejudice to their future elaboration within the framework of progressive development of the international law of armed conflict: . . . [i]n the conduct of military operations during armed conflicts, a distinction must be made at all times between persons actively taking part in the hostilities and civilian populations." (quoting G.A. Res. 2675, U.N. GAOR, 25th Sess., Supp. No. 28, U.N. Doc. A/8028 (Dec. 9, 1970). *See also Nuclear Weapons*, *supra* note 33, ¶ 79 (distinction is one of the "intransgressible principles of international customary law"); CIHL, *supra* note 54, at 3–8; Abella v. Argentina, Case 11.137, Inter-Am. C.H.R., Report No. 55/97, OEA/Ser.L/V/II.95, doc. 7 rev. ¶¶ 177–178 (1997).

56. AP I, *supra* note 36, art. 51(2).

57. *Id.*, art. 85.

58. *See* Rome Statute of the International Criminal Court arts. 8(2)(b)(i), 8(2)(b)(ii), 8(2)(b)(iv), 8(2)(b)(v), 8(2)(b)(vi), 8(2)(e)(i), 8(2)(e)(ii), 8(2)(e)(iv), July 17, 1998, 2187 U.N.T.S. 90, *available at* http://untreaty.un.org/cod/icc/statute/english/rome_statute(e).pdf.

mand and abiding by the law of armed conflict.[59] Members of the regular armed forces of a government not recognized by the opposing party and civilians participating in a *levée en masse* also qualify as combatants in international armed conflict.[60] Combatants can be attacked at all times and enjoy no immunity from attack, except when they are *hors de combat* due to sickness, wounds or capture. To the extent that a State is responding to cyber threats or attacks by non-State actors in an international armed conflict, the first question will be whether the non-State actor falls within one of these combatant categories. Although unlikely, if they do, the non-State actors will be targetable at all times on the basis of their status as combatants. Assuming they do not, then the non-State actors remain civilians and retain their immunity from attack except at such times as they directly participate in hostilities. Each of these considerations will be addressed below. For each category the analysis with regard to non-international armed conflict applies in international armed conflict as well.

In non-international armed conflicts, which are most often between a State and a non-State entity, but can be between or among multiple non-State groups, there is no combatant status; thus operationalizing distinction relies on alternative means of distinguishing those who are fighting from those who are not. A significant question is therefore whether members of opposition groups are simply civilians fighting against the government or constitute an organized force distinct from the civilian population.[61] If they are civilians, then they are immune from attack except when directly participating in hostilities, like all other civilians. If they are members of an organized armed force, then they are targetable at all times, regardless of whether they are engaged in hostilities at the time.[62] In general, the term

59. GC III, *supra* note 36, art. 4(A)(2).

60. *Id.*, arts. 4(A)(3), 4(A)(6).

61. For a comprehensive discussion of the status of persons fighting against the government in a non-international armed conflict, see Michael N. Schmitt, *The Status of Opposition Fighters in a Non-International Armed Conflict*, *in* NON-INTERNATIONAL ARMED CONFLICT IN THE TWENTY-FIRST CENTURY 119 (Kenneth Watkin & Andrew J. Norris eds., 2012) (Vol. 88, U.S. Naval War College International Law Studies).

62. *See* JIMMY GURULÉ & GEOFFREY S. CORN, PRINCIPLES OF COUNTER-TERRORISM LAW 70–76 (2011) (discussing the rules governing targeting of enemy forces in international and non-international armed conflict and noting that (1) "a member of an enemy force . . . is presumed hostile and therefore presumptively subject to attack" in international armed conflict and (2) "subjecting members of organized belligerent groups to status based targeting pursuant to the LOAC as opposed to civilians who periodically lose their protection from attack seems both logical and consistent with the practice of states engaged in non-international armed conflicts"); NILS MELZER, INTERNATIONAL COM-

"organized armed group"—used to describe the non-State party to a conflict—refers specifically to the military wing of a non-State actor, essentially the functional equivalent of the government armed forces. Organized armed groups "recruit their members primarily from the civilian population but develop a sufficient degree of military organization to conduct hostilities on behalf of a party to the conflict, albeit not always with the same means, intensity and level of sophistication as State armed forces."[63] A commonly used, but still contentious, method for identifying members of organized armed groups is the notion of continuous combatant function, introduced in the ICRC's *Interpretive Guidance on the Notion of Direct Participation in Hostilities*. As the *Guidance* explains, "membership [in an organized armed group] must depend on whether the continuous function assumed by an individual corresponds to that collectively exercised by the group as a whole, namely the conduct of hostilities on behalf of a non-State party to the conflict."[64] Although there remains extensive debate regarding the concept of continuous combat function and the identification of members of an organized armed group, such debate is outside the scope of this article. Rather, for the purposes of the instant analysis, it is sufficient to focus on the fundamental distinction that is recognized between members of an organized armed group and civilians.

The cyber-specific issues in this area are quite similar to those raised in the earlier discussion regarding the nature of organization for purposes of classifying an armed conflict. If individuals who engage in cyber attacks against the State are part of an organized armed group, they will be targetable at all times. The challenge lies in identifying an organized group that operates solely in the cyber realm and, as a second step, in identifying the members of that group so as to make targeting decisions appropriately.

A second category of individuals who can be targeted lawfully under LOAC is civilians who take direct part in hostilities. Such persons are legitimate targets of attack during and for such time as they engage directly in hostilities.[65] In certain limited circumstances, therefore, civilians may be

---

MITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 16–17 (2009), *reprinted in* 90 INTERNATIONAL REVIEW OF THE RED CROSS 991, 996 (2008), *available at* http://www.icrc. org/eng/assets/files/other/icrc-002-0990.pdf (stating that organized armed groups are targetable based on status in non-international armed conflict) [hereinafter INTERPRETIVE GUIDANCE].

63. INTERPRETIVE GUIDANCE, *supra* note 62, at 32.

64. *Id.* at 33.

65. AP I, *supra* note 36, art. 51(3).

directly and intentionally targeted during hostilities. Thus, "[t]he principle of distinction acknowledges the military necessity prong of [the law's] balancing act by suspending the protection to which civilians are entitled when they become intricately involved in a conflict."[66] In recent years, courts and commentators have struggled to define the concept of direct participation in hostilities and develop parameters for understanding when civilians—as the term is traditionally used—become legitimate targets by reason of such participation.[67] A detailed analysis of direct participation is outside the scope of this article; it is sufficient to define direct participation in hostilities as acts intended to harm the enemy or the civilian population in a direct or immediate manner, therefore making the actor a legitimate target of attack for the purposes of distinction within LOAC. The analysis here will focus specifically on identifying direct participation in the cyber arena.

Some examples of cyber acts that could constitute direct participation in hostilities include writing and executing malicious code, launching distributed denial of service attacks, providing malware or other cyber tools to a party to the conflict, or other forms of cyber attack. More complicated questions involve the status of persons who engage in cyber operations that do not qualify as cyber attacks but contribute directly to cyber operations and cyber attacks, such as hacking into an enemy computer to gather intelligence to be used in the launching of an attack or planting a worm in software that breaks down defenses, thus enabling a subsequent attack to

66. Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 HARVARD NATIONAL SECURITY JOURNAL 5, 12 (2010).

67. *See, e.g.*, HCJ 769/02 Public Committee against Torture in Israel v. Government of Israel 2006 (2) PD 459 [2006] (Isr.), *reprinted in* 46 INTERNATIONAL LEGAL MATERIALS 373, *available at* http://elyon1.court.gov.il/Files_ENG/02/690/007/a34/02007690.a34.pdf [hereinafter *Targeted Killings*]; Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Judgment, ¶ 616 (Int'l Crim. Trib. for the former Yugoslavia July 15, 1999). *See generally* CIHL *supra* note 55, at 2–9; Jason Callen, *Unlawful Combatants and the Geneva Conventions*, 44 VIRGINIA JOURNAL OF INTERNATIONAL LAW 1025 (2004); Derek Jinks, *Protective Parity and the Laws of War*, 79 NOTRE DAME LAW REVIEW 1493, 1495–1501 (2004); Jann K. Kleffner, *From "Belligerents" to "Fighters" and Civilians Directly Participating in Hostilities—On The Principle of Distinction in Non-International Armed Conflicts One Hundred Years After the Second Hague Peace Conference*, 54 NETHERLANDS INTERNATIONAL LAW REVIEW 315 (2007); INTERPRETIVE GUIDANCE, *supra* note 63; W. Hays Parks, *Air War and the Law of War*, 32 AIR FORCE LAW REVIEW 1 (1990); Michael N. Schmitt, *Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees*, 5 CHICAGO JOURNAL OF INTERNATIONAL LAW 519, 522–36 (2005); Kenneth W. Watkin, *Combatants, Unprivileged Belligerents and Conflict in the 21st Century*, 1 ISRAEL DEFENSE FORCES LAW REVIEW 69 (2003).

be successful.[68] In any of these or other situations, identifying direct participation requires that the act in question cause harm directly to the opposing side or to civilians and that it have a nexus to the armed conflict.[69]

Some of the already challenging conceptual issues in applying direct participation in hostilities in kinetic operations become even thornier in the framework of cyber operations. Beyond the identification of the types of acts or contributions that fit within the notion of direct participation, the "for such time as" component of direct participation proves to be especially complex. It is generally accepted that acts preparatory to or returning from a deployment are considered to be part of the act that constitutes direct participation in hostilities.[70] Here, an initial question must be how to determine which acts constitute the actual attack, which are considered preparatory to execution or deployment, and which are too attenuated to fit within the paradigm. The malware, worm or other trigger of a cyber attack will often be inserted into the relevant software, server or network well in advance of the actual time of the attack or eventual consequences, which naturally raises the question of when the individual launching the attack is directly participating in hostilities. Is it only when designing and inserting the malware? When the attack is actually launched, as well for the duration of the attack? And in the instantaneous world of virtual communications and cyber operations, identifying the conduct that should be considered to be preparatory to or returning from execution or deployment simply may not be relevant or possible. As a result, the same questions of a revolving door[71]—the farmer by day, fighter by night example—arise in cyber as in other types of operations, but perhaps with greater urgency and even less discernibility.

---

68. *See* Yoram Dinstein, *The Principle of Distinction and Cyber War in International Armed Conflicts*, 17 JOURNAL OF CONFLICT AND SECURITY LAW 261, 263 (2012) (stating that the following do not qualify as cyber attacks because they do not produce violent effects: hacking into an enemy computer for intelligence-gathering purposes, breaking through a computer's firewall, planting a worm in digital software, extracting secret data, gaining control over codes and disrupting communications).

69. *See, e.g.*, INTERPRETIVE GUIDANCE*, supra* note 62, at 46 (three key components of direct participation are the threshold of harm, direct causation and belligerent nexus). *See also* David Turns, *Cyber Warfare and the Notion of Direct Participation in Hostilities*, 17 JOURNAL OF CONFLICT AND SECURITY LAW 279 (2012) (providing a chart analyzing ten different types of cyber acts within the framework of threshold of harm, direct causation and belligerent nexus).

70. INTERPRETIVE GUIDANCE*, supra* note 62, at 65.

71. *See Targeted Killings*, *supra* note 67.

Finally, the requirement that there be a belligerent nexus, a connection between the relevant act and the ongoing armed conflict, can certainly pose particular challenges in the cyber arena, where it can be difficult in some situations to distinguish hacking, cyber crime and cyber espionage from more conflict-related cyber acts. As a result, States considering responses to cyber activity by non-State actors will need to rely on extensive cooperation between the law enforcement, intelligence and military communities in order to ensure an effective and lawful response to cyber acts and cyber threats.

These distinctions between individuals—whether members of organized armed groups, civilians directly participating in hostilities or innocent civilians—are relevant not only during combat operations, when one side has to make determinations about who and what is targetable, who can be detained, and who and what must be protected. They are also significant—indeed foundational—considerations in any post-conflict accountability process. For example, the crime of attacking civilians depends, at first, on the identification of the victims as civilians who are entitled to immunity from attack (i.e., they are not directly participating in hostilities at the time of the attack). In a prosecution for attacks on civilians during non-international armed conflict, a defendant is likely to argue that the victims were not civilians but rather were members of the opposing forces. As noted above with regard to responses to non-State actors during the course of conflict, the necessary linkage between the cyber operations of the individuals who were attacked and the armed conflict will be the central issue in the accountability paradigm as well. Crimes and criminal activity persist and often flourish during armed conflict, but that does not mean that all crimes and all criminals should be prosecuted within a LOAC framework. Rather, there must be a nexus between the act and the armed conflict in order for international criminal accountability to attach.[72] Here, the ability to distinguish between cyber crime and other "non-war" cyber activities, to identify which cyber activities are linked to an ongoing conflict and which are simply opportunistic criminal activity, is a prerequisite to any accountability efforts after the conflict.

72. Prosecutor v. Kunarac, Case No. IT-96-23/1-T, Judgment, ¶ 58 (Int'l Crim. Trib. for the former Yugoslavia Feb. 22, 2001).

2. Proportionality and Precautions

Legal analysis does not end with identification of a legitimate target. Rather, the attacking party must then assess whether the attack meets the requirements of the principle of proportionality and take other necessary precautions to comply with LOAC's mandates. Detailed specifically in Additional Protocol I, these obligations apply as a matter of customary international law in all conflicts, whether international or non-international. The primary issue with regard to State responses to cyber attacks or threats from non-State actors is, as explored in greater detail above, the challenge of identifying which individuals and objects are legitimate targets for attack and which are civilian in nature and protected from attack under LOAC. This subsection will, therefore, simply provide a brief explanation of the fundamental obligations of proportionality and precautions that apply to any cyber attack launched against non-State actors in the course of an armed conflict, without delving deeply into the broader issues relevant to proportionality and precautions in the cyber context that would arise across the spectrum of conflict.[73] One example is the cascading effects that cyber attacks can have and how to analyze such effects for the purposes of proportionality.

The principle of proportionality requires that parties refrain from attacks in which the expected civilian casualties will be excessive in relation to the anticipated military advantage gained. Additional Protocol I contains three separate statements of the principle of proportionality. The first appears in Article 51, which sets forth the basic parameters of the obligation to protect civilians and the civilian population, and prohibits any "attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[74] This language demonstrates that Additional Protocol I contemplates incidental civilian casualties. It appears again in Articles 57(2)(a)(iii)[75]

73. For an analysis of precautions and proportionality in the cyber context, see Eric Talbot Jensen, *Cyber Attacks: Proportionality and Precautions in Attack*, 89 INTERNATIONAL LAW STUDIES 198 (2013).

74. AP I, *supra* note 36, art. 51(5)(b).

75. *Id.*, art. 57(2)(a)(iii) ("With respect to attacks, the following precautions shall be taken: [t]hose who plan or decide upon an attack shall . . . [r]efrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated . . . .").

and 57(2)(b),[76] which refer specifically to precautions in attack. Proportionality is not a mathematical concept, but rather a guideline to help ensure that military commanders weigh the consequences of a particular attack and refrain from launching attacks that will cause excessive civilian deaths or damage to civilian property.

LOAC also mandates that all parties take certain precautionary measures to protect civilians. In many ways, the identification of military objectives and the proportionality considerations are, of course, precautions. But the obligations of the parties to a conflict to take precautionary measures go beyond that. Beginning at the broadest level, Article 57(1) of Additional Protocol I states, "In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects."[77] This provision is a direct outgrowth of and supplement to the Basic Rule in Article 48, which mandates that all parties distinguish between combatants and civilians and between military objects and civilian objects. The practical provisions forming the major portion of Article 57 discuss precautions to be taken specifically when launching an attack. First, parties must do everything feasible to ensure that targets are military objectives. Doing so helps to protect civilians by limiting attacks to military targets, thus directly implementing the principle of distinction. Second, they must choose the means and methods of attack with the aim of minimizing incidental civilian losses and damage. For example, during the 1991 Persian Gulf War, "pilots were advised to attack bridges in urban areas along a longitudinal axis. This measure was taken so that bombs that missed their targets—because they were dropped either too early or too late—would hopefully fall in the river and not on civilian housing."[78] Another common method of taking precautions is to launch attacks on particular targets at night when the civilian population is not on the streets or at work, thus minimizing potential casualties. In addition, when choosing between two

76. *Id.*, art. 57(2)(b) ("An attack shall be cancelled or suspended if it becomes apparent that the objective is not a military one or is subject to special protection or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated . . . .").

77. *Id.*, art. 57(1).

78. Jean-François Quéguiner, *Precautions Under the Law Governing the Conduct of Hostilities*, 88 INTERNATIONAL REVIEW OF THE RED CROSS 793, 801 (2006) (noting that this angle of attack "also means that damage would tend to be in the middle of the bridge and thus easier to repair") (citing Michael W. Lewis, *The Law of Aerial Bombardment in the 1991 Gulf War*, 97 AMERICAN JOURNAL OF INTERNATIONAL LAW 481 (2003)).

possible attacks offering similar military advantage, parties must choose the objective that offers the least likely harm to civilians and civilian objects. Finally, Article 57(2)(c) requires attacking parties to issue an effective advance warning "of attacks which may affect the civilian population, unless circumstances do not permit."[79]

The issues of attribution and distinction discussed above are equally relevant with regard to proportionality and precautions. Proportionality's obligations only attach when some civilian casualties, injury or damage are expected to occur; making such determinations relies first on the ability to determine that some of the potential victims of the attack will be civilians. Similarly, the various precautionary obligations demand an ability to distinguish between military and civilian objects and to identify where civilians are located, if warnings are needed, and how to provide such warnings and other protections against the effects of attacks. In the course of an armed conflict with a non-State armed group—whether a more traditional armed group or one that fights primarily with cyber weapons—the State must develop and use the capacity to identify and differentiate between civilian and military persons and objects, not only for the purposes of identifying whom it is fighting against but also for the purposes of protecting those who are uninvolved in the conflict and merit protection under LOAC.

IV. RHETORIC AND ITS CONSEQUENCES IN OPERATIONS AGAINST NON-STATE ACTORS

In considering the parameters of State responses to cyber threats from non-State actors, it is important to recognize the role that rhetoric does and can play in this arena. Terms such as "cyber war," "cyber warfare" and "cyber attack" are used to describe a broad array of activities, many of which fall outside the scope of the types of attacks discussed here, the types of attacks that trigger the *jus ad bellum* or attacks as that term is used within LOAC. For example, an early definition of cyber warfare, but one still in regular use, is "any operation that disrupts, denies, degrades, or destroys information resident in computers or computer networks."[80] In another study, the authors split cyber warfare into five general varieties, ranging from the mildest to the most severe: (1) web vandalism, (2) disinformation campaigns, (3) gathering secret data, (4) disruption in the

79. AP I, *supra* note 36, art. 57(2)(c).

80. WALTER GARY SHARP SR., CYBERSPACE AND THE USE OF FORCE 132 (1999).

field and (5) attacks on critical national infrastructure.[81] The use of terms that sound like "war" but are in fact much broader in scope than the corresponding legal terms and definitions can have significant consequences for the application of the law, the execution of operations and the protection of persons and property.

Counterterrorism policy over the past decade offers a prime example of the impact rhetoric can have on the development and implementation of the law. The rhetoric of the "war on terror" facilitated and encouraged the growth of authority without the corresponding obligation in many cases. For example, the drone campaign in Pakistan, indefinite detention, prosecution of crimes such as conspiracy or material support for terrorism in military commissions and other practices have raised significant questions about the application of domestic and international law to counterterrorism operations, the long-term impact on executive authority and the use of national security as a "trump card" in the face of legal obstacles or challenges. In addition, layering rhetoric on top of the law has affected the application and implementation of key bodies of law, such as human rights law, LOAC and various domestic legal regimes relevant to national security and counterterrorism.[82] Over the course of several years, the mix of counterterrorism operations and military operations, and a rhetoric of war that subsumed both, helped lead to minimized rights and magnified executive powers.

Just as the rhetoric of war subsumed a wide variety of counterterrorism measures within the concept of a "war on terror" and ultimately had a profound effect on both law and policy with respect to counterterrorism and war, so the potential for similar consequences in the cyber arena exists as well. Cyber activities can span a continuum of "bad activity" from cyber crime to cyber espionage to cyber terrorism an all the way to cyber attacks and cyber war. Not all of these acts fit within the paradigm of international law governing the use of force or the LOAC regime, as detailed earlier in this article. As a result, it is essential to differentiate between actors with "war" intentions and those with malicious or criminal intentions, especially when assessing the appropriate response to non-State actors engaged in

---

81. *See* Center for the Study of Technology and Society, *Special Focus: Cyberwarfare,* http://web.archive.org/web/20061205020720/tecsoc.org/natsec/focuscyberwar.htm (2001).

82. *See generally* Laurie R. Blank, *The Consequences of a "War" Paradigm for Counterterrorism: What Impact on Basic Rights and Values?*, 46 GEORGIA LAW REVIEW 719 (2012).

some type of damaging cyber conduct.[83] Understanding the impact of certain rhetorical choices is equally important. For example, the term "cyber attack" is regularly used in the mass media to denote an extremely wide range of cyber conduct, much of which falls well below the threshold of an "armed attack" as understood in the *jus ad bellum* or an attack as defined in LOAC for purposes of triggering the obligations of distinction, proportionality and precautions. Rhetoric that uses a terminology of war, like "cyber war" or "cyber attack," can create situations in which a State has fewer obstacles to an aggressive response to a non-State actor's cyber threats or cyber conduct, stretching or overstepping the relevant legal boundaries. In this way, such rhetoric poses a serious risk of elevating or escalating an apparently hostile action to the status of war or conflict when, in the absence of such rhetoric, it would be more appropriately handled or countered within the criminal system or other non-forceful paradigm.

The interplay between law and rhetoric thus forms an important backdrop to the analysis of the international legal norms that govern how a State can respond to cyber threats from non-State actors. Rhetoric that opens the door to overly broad responses necessitates an understanding of the relevant legal paradigms, the boundaries between them and the fundamental principles that guide their application. Use of terms like "war" and "attack" for a much wider array of activities also facilitates a blurring of the lines between relevant and applicable legal frameworks, which can have a detrimental effect on both individual rights and the development of the law. With regard to cyber threats and cyber attacks, both the *jus ad bellum* and LOAC help shape the parameters of lawful and effective action in response to non-State actors, not only by guiding the appropriate conduct when force may lawfully be used or during armed conflict, but also by delineating the dividing line between crime and war and between self-defense and law enforcement.

---

83. *See, e.g.*, Nils Melzer, *Cyber Operations and* Jus in Bello, DISARMAMENT FORUM, no. 4, 2011, at 3, *available at* http://www.unidir.org/pdf/articles/pdf-art3164.pdf ("Applied to the more specific context of cyber operations, this means that the use of the terms 'cyberwar,' 'cyberwarfare,' 'cyberhostilities,' and 'cyberconflict' should be restricted to armed conflicts within the meaning of [international humanitarian law]. Indeed, security threats emanating from cyberspace that do not reach the threshold of armed conflict can be described as 'cybercrime,' 'cyber operations,' 'cyberpolicing' or, where appropriate, as 'cyberterrorism' or 'cyberpiracy,' but should not be referred to with terminology inviting doubt and uncertainty as to the applicability of the law of armed conflict.").

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Anticipatory Self-Defense in the Cyber Context

Terry D. Gill and Paul A. L. Ducheine

89 INT'L L. STUD. 438 (2013)

Volume 89 2013

Anticipatory Self-Defense in the Cyber Context

Terry D. Gill and Paul A. L. Ducheine[*]

I. INTRODUCTION

This article will examine the question of whether the right of self-defense under contemporary international law permits a State to react to an imminent or potential armed attack carried out by digital means in two circumstances. First, as an attack occurring in conjunction with, or as an adjunct to, a conventional kinetic armed attack intended to neutralize the target State's defensive and command and control systems. Second, as an attack—independent of any use of kinetic force—intended to cause significant human casualties, physical damage or large-scale disruption in the target State. While the former scenario is probably considerably more likely than the latter scenario, both will receive attention. The applicable law is the same in either scenario, although there are some potentially significant differences in the modalities of its application, primarily in the identification of the attacking party and in gauging the level of the response if an attack was conducted wholly in the digital domain.

* Terry D. Gill is Professor of Military Law, University of Amsterdam and Netherlands Defence Academy. Paul A. L. Ducheine is Associate Professor of Cyber Operations, Netherlands Defence Academy, and Senior Guest Lecturer and Research Associate, University of Amsterdam.

A. Starting Points

This article assumes a number of issues are "givens" for the purposes of this discussion.

First, that any use of force at the international level is, as a matter of law, governed by the international law on the use of force, irrespective of the manner in which the force is conducted and carried out.[1]

Second, while the use of force in the cyber context poses certain challenges in *how* and *when* the existing legal framework regulating the use of force can be applied, it is capable, in principle, of being applied to any type of force that can be qualified as such. Consequently, that it can be applied to computer-based attacks just as it can be applied to other forms of both kinetic and non-kinetic force, such as bacteriological, radiological and chemical weapons, whether used in conventional warfare or in terrorist assaults.[2] While the specific characteristics of cyber attack differ in some important respects from conventional kinetic attack and most forms of what is loosely referred to as "cyber attack" do not qualify as either a use of force or armed attack, those that do cause—or are intended to cause—significant loss of life, physical destruction or long-term disruption of a State's vital infrastructure could constitute an armed attack. Hence, the contemporary legal framework is applicable as a matter of law and potentially relevant in the cyber context. There are neither legal nor practical reasons to assume that the existing international legal framework governing the use of force in the cyber realm is irrelevant, inadequate or incapable of being applied without clear and convincing evidence so indicating.

Third, there are no separate rules and legal principles for the use of force in the cyber context. Therefore, notions such as "use of force," "armed attack," "necessity," "immediacy" and "proportionality" are no different in the cyber context than in the physical world, although the modalities of their application might well differ to some extent. Likewise, the rules relating to attribution of an attack to a particular State or non-State entity

1. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 39 (July 8).

2. Paul Ducheine, Joop Voetelink, Jan Stinissen & Terry Gill, *Towards a Legal Framework for Military Cyber Operations*, *in* CYBER WARFARE: CRITICAL PERSPECTIVES 101 (Paul Ducheine, Frans Osinga & Joseph Soeters eds., 2012).

do not cease to be applicable when the attack is carried out by cyber means.[3]

Fourth, self-defense of States at the international level is relevant only to unlawful uses of force originating outside a State's territory that rise to the level of an armed attack. This means that any other type of activity, whether it involves a degree of force below this threshold or constitutes criminal conduct or a violation of other national or international legal rules not related to the use of force, falls outside the scope of those actions to which States may respond in self-defense. Therefore, cyber criminal activity, cyber (corporate) espionage and various other forms of unauthorized penetration, theft of data and sabotage of computer systems, whether public or private, that do not fit within the definition of armed attack are not subject to the law relating to self-defense and will not be addressed in this article. Such activities may well constitute unlawful intervention or other violations of international and national law, but the violations do not give rise to the right of self-defense when carried out in the physical world. There are no compelling reasons why this should be different in the cyber domain.

B. Structure

Section II will set out the essential nature and purpose of the right of self-defense, and examine its scope and the legal conditions governing its exercise under both the UN Charter and customary international law. Since the law regulating the use of force and the exercise of the right of self-defense are taken to be applicable, relevant and based upon the same rules, conditions and principles in the cyber context as in the physical domain, it is essential to set out this legal framework as clearly and succinctly as possible in order to determine the conditions and modalities of the exercise of self-defense. In particular the legality of anticipatory self-defense under contemporary international law is reviewed. To the extent that anticipatory self-defense is permitted or, alternatively, seen as lacking a legal basis within the right of self-defense in general, this will be relevant to its possible application in responding to an imminent cyber armed attack.

---

3. This is the approach taken by the International Court of Justice (ICJ) in its *Nuclear Weapons* advisory opinion, *supra* note 1, ¶¶ 37–50, 244–47, and unanimously by the Group of Experts responsible for the TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013).

Following this summary of the current legal framework regulating the use of force and the exercise of self-defense, we turn in Section III to its application in the cyber context. The modalities of a cyber armed attack will first be examined. We will then look into the particular challenges of applying the legal framework governing the exercise of self-defense, in particular anticipatory self-defense, in the cyber context. While the applicable law is the same, there are specific challenges and modalities involved in applying it to the cyber context, principally, in situations when cyber weapons are employed in the absence of more traditional kinetic force. In such situations, the challenges posed include ascertaining the source of the attack and identity of the attacker, determining potential consequences of the attack and gauging the response in terms of necessity, immediacy and proportionality.

In Section IV, we draw a number of conclusions and provide a clear answer to the question of whether anticipatory action in self-defense would be a legal response, and, to the extent it is, what conditions and limitations of a general and specific nature are relevant.

II. THE LEGAL FRAMEWORK GOVERNING THE EXERCISE OF THE RIGHT OF SELF-DEFENSE.

This section will first deal with the essence and legal basis of self-defense and then discuss the criteria pertaining to it as found in the UN Charter and customary international law.

A. Essence and Dual-Legal Basis of Self-Defense

The right of self-defense under international law is the right of a State to repel or, if necessary, overcome an unlawful use of force amounting to an armed attack.[4] That is what characterizes it and sets it apart from other uses of force, whether lawful (e.g., action undertaken by or with the authorization of the UN Security Council to maintain or restore international peace and security or as a law enforcement measure in the domestic legal con-

4. *See* Terry D. Gill, *Legal Basis of the Right of Self-Defence under the UN Charter and under Customary International Law*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS 187, 187–88 (Terry D. Gill & Dieter Fleck eds., 2010).

text), or unlawful (e.g., uses of force that do not have a recognized legal basis).[5]

Self-defense is both an *inherent* right of States under customary international law and an exception to the prohibition on the use of force as laid out in Article 2(4) of the UN Charter. The inclusion of the right of self-defense within the Charter had and has a dual purpose: recognition of the preexisting right of States under customary international law and integration of the right of self-defense into the Charter system of collective security in order to provide an unequivocal basis for collective self-defense.[6] Any legal assessment of self-defense must take into account the Charter's substantive and procedural requirements, as well as the criteria for the exercise of this right under customary international law.

The two sources are complementary, and in no way conflict with each other when applied with this understanding. The starting point for any interpretation of how they interact is to examine the Charter text, considering, when necessary, the intentions of the drafters, as well as the object and purpose of the entirety of Charter provisions related to the use of force and the maintenance of international peace and security. Additionally, the nature and conditions of self-defense under customary international law are crucial to a correct interpretation and application of the right, since the Charter both recognizes its customary nature and does not seek to supplant or override the conditions laid down in customary law, except in so far as explicitly provided for in the Charter. The Charter drafters did not set out to recast the right of self-defense from scratch; instead they recognized the existence of the right and embedded it in the Charter system. This means that the right as it existed at the time the Charter came into force is the

5. The legal character of self-defense is set out and analyzed in D. W. BOWETT, SELF-DEFENCE IN INTERNATIONAL LAW 3–25 (1958); IAN BROWNLIE, INTERNATIONAL LAW AND THE USE OF FORCE BY STATES 251 (1963); YORAM DINSTEIN, WAR, AGGRESSION AND SELF- DEFENCE 187–93 (5th ed. 2012); and C.H.M. Waldock, *The Regulation of the Use of Force by Individual States in International Law*, 41 RECUEIL DES COURS 455, 455–68 (1952). With regard to the premise that self-defense is a lawful response to unlawful force, see DINSTEIN, *supra* note 5, at 190 (quoting the decision of the U.S. Military Tribunal in United States v. Ernst von Weizsäcker et al., 14 TRIALS OF WAR CRIMINALS BEFORE THE NUERNBERG MILITARY TRIBUNALS 329 (1949)).

6. The inclusion of Article 51 in the UN Charter came at a relatively late stage in the negotiations leading to the Charter's adoption. It was added at the behest of Latin American States, which wanted to safeguard the right of mutual assistance arrangements in the event of attack. *See* BOWETT, *supra* note 5, at 182–83; LELAND GOODRICH, EDVARD HAMBRO & ANNE SIMONS, CHARTER OF THE UNITED NATIONS 342–44 (1969); Waldock, *supra* note 5, at 503–4.

right that is referred to as "inherent" in Article 51. In the absence of clear evidence to the contrary, there is no reason to assume that there was any intention to substantially alter the content of the right of self-defense in either the text of the Charter itself or in the negotiations leading to the incorporation of the right into the Charter. Therefore, since the Charter is silent on many aspects of the content of the right, an assessment of an invocation of self-defense must take into account the conditions contained in the Charter and customary law, as well as the factual considerations surrounding its invocation.[7]

B. Conditions Laid Out in the Charter

1. Armed Attack

The Charter predicates the exercise of the right of self-defense on the occurrence of an "armed attack." We will also examine the temporal dimension of an armed attack (that is, at what point in time does it occur), but for now we will concentrate on the question of what is an armed attack.

The Charter provides little or no guidance as to what constitutes an armed attack. To ascertain its meaning, we must look for guidance to customary law and supplementary sources, such as international jurisprudence. Based on these, an armed attack is considered to be a use of force originating outside the target State's territory that rises above the level of a small-scale, isolated armed incident or criminal activity, and which is directed against a State's territory, its military vessels or aircraft in international waters or airspace or lawfully present in another State's territory, or, in certain situations directed against its nationals located abroad.[8] It could also in-

---

7. The dual-legal basis of self-defense and the complementary relationship of the Charter and customary law were acknowledged by the ICJ in its *Nicaragua* decision. *See* Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S), 1986 I.C.J. 14, ¶ 94 (June 27) [hereinafter *Nicaragua Judgment*]. The continued relevance of a preexisting rule of customary law in the absence of evidence of the emergence of a newer one regulating the same issue follows from general legal methodology and the doctrine of interpretation of legal sources. *See* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 3–4 (4th ed. 1990); 1 R.Y. JENNINGS & ARTHUR WATTS, OPPENHEIMS'S INTERNATIONAL LAW 25–26 (9th ed. 1992); Rudolf Bernhardt, *Customary International Law*, *in* 7 ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW 61–62 (Rudolf Bernhardt ed., 2003).

8. The requirement that an armed attack originate from a source located or controlled outside a State's territory is generally acknowledged and non-controversial, as are the listed objects, which, if attacked, would constitute an armed attack, with the exception of a

clude a non-kinetic attack involving a use of force that resulted in more than nominal human casualties, or significant physical damage or destruction to either military or civilian objects.

Additionally, an armed attack could arguably include a cyber attack directed against a State's critical infrastructure, provided the cyber attack had the potential to severely cripple a State's ability to carry out and ensure the conducting of essential State functions or severely undermine its economic, political and social stability for a prolonged period of time. A number of States have adopted this position in their national cyber security strategies and many experts concur that an attack of this nature could potentially amount to a use of force rising to the level of an armed attack, although opinion is sharply divided.[9]

State´s nationals located abroad. The latter is controversial, with some authorities rejecting the position that an attack against a State's nationals abroad constitutes an armed attack, while others take the view that protection of nationals falls within the customary right of self-defense. There is a middle view which accepts that if nationals of a State are the target of threats to their lives or physical safety in order to obtain concessions or a change of policy from their parent State, this can constitute an armed attack. These views and the present authors' position are set out in Terry D. Gill & P.A.L. Ducheine, *Rescue of Nationals Abroad*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS, *supra* note 4, at 217–19. On armed attack generally, see TOM RUYS, "ARMED ATTACK" AND ARTICLE 51 OF THE UN CHARTER: EVOLUTIONS IN CUSTOMARY LAW AND PRACTICE (2010).

9. The cyber strategies of several nations acknowledge the possibility of treating an attack that results in human casualties and/or significant physical damage as an armed attack justifying the exercise of self-defense. *See, e.g.,* U.S. Department of Defense, Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, at 4, 9 (2011), *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAASection 934Report_Forwebpage.pdf. The Advisory Council on International Affairs and the Committee on Issues of Public International Law in the Netherlands issued a 2011 joint report, "Cyber Warfare," that was adopted by the Netherlands Government. In this report, both a digital attack with comparable effects to those of a traditional kinetic attack and an attack upon critical infrastructure that produces severe and long-term effects were deemed as potentially triggering the right of self-defense. *See* ADVISORY COUNCIL ON INTERNATIONAL AFFAIRS & ADVISORY COMMITTEE ON ISSUES OF PUBLIC INTERNATIONAL LAW, CYBER WARFARE 21 (2011), *available at* http://www.aiv-advies.nl/ContentSuite/upload/aiv/doc/webversie__AIV77CAVV_22_ENG.pdf. In the Group of Experts that prepared the *Tallinn Manual,* there was unanimity that a cyber attack with comparable scale and effects to that of a kinetic attack which results in human casualties and physical damage or destruction could constitute an armed attack. The experts were divided, however, on the question whether a cyber attack without such physical

In that regard, it must be pointed out that there is currently insufficient State practice and official policy statements to conclude with certainty that an attack of this nature would amount to an armed attack in the absence of potential loss of life, physical injury or property damage. In the opinion of the authors, such an attack could so qualify under certain conditions. If the attack caused either physical damage or human injury of any significance, it would definitely so qualify. Additionally, even in the absence of physical injury or damage it could, in our opinion, constitute an armed attack, provided the potential disruption of a State's essential functions or stability was severe, long-term and incapable of being remedied within a reasonable time period.

An armed attack can be conducted in various ways, ranging from full-scale invasion to a series of small-scale uses of force conducted by the same author against the same target State that are reasonably connected in geographic and temporal terms and constitute what is, in effect, a phased armed attack.[10]

Some of these modes of attack are more relevant in the cyber context than others. This will receive further attention in a subsequent section.

2. Authorship of Armed Attack

There is general agreement that the potential authors of an armed attack include a State's armed forces and organized armed groups acting under the control of a State. Mere political or ideological sympathy, or diplomatic, logistical or material support for the organized armed group would not, in principle, constitute the requisite level of State involvement to be considered participation in the attack. If, however, a State's material or logistical support was substantial, it could potentially reach that level.[11]

---

effects, even one resulting in severe long-term disruption to critical infrastructure, could constitute an armed attack. TALLINN MANUAL, *supra* note 3, cmt. to rule 13, ¶¶ 6–9.

10. This is often referred to as the "accumulation of events" theory. It is also referred to as a "pin-prick" armed attack or "*Nadelstichtaktik*." *See, e.g.*, Yehuda Z. Blum, *State Response to Acts of Terrorism*, 19 GERMAN YEARBOOK OF INTERNATIONAL LAW 223 (1976); Paul Ducheine & Eric Pouw, *Operation Change of Direction: A Short Survey of the Legal Basis and the Applicable Legal Regimes*, *in* NETHERLANDS ANNUAL REVIEW OF MILITARY STUDIES—COMPLEX OPERATIONS: STUDIES ON LEBANON (2006) AND AFGHANISTAN (2006–PRESENT) 51, 61–63 nn. 49–82 (Michiel de Weger et al. eds., 2009).

11. *Nicaragua Judgment*, *supra* note 7, ¶¶ 195, 103. The views of one of the present authors on substantial involvement are set out in P.A.L. Ducheine & E.H. Pouw, *Legitimizing the Use of Force*, *in* MISSION URUZGAN—COLLABORATING IN MULTIPLE COALITIONS FOR

In addition to these two uncontroversial categories, there is increasing acceptance that an armed attack is capable of being carried out by an armed group not under the control of a State, but which instead acts autonomously with greater or lesser degrees of State tolerance and support that fall short of control or even influence.[12] Although some legal experts and court decisions cast doubt on whether such a group could carry out an armed attack, the better opinion in our view is that there are good grounds for not ruling out this possibility. Nothing in the Charter text relating to self-defense excludes it and this possibility has long been recognized in customary international law. There is also considerable recent State and international practice supporting this proposition and a wide degree of acceptance on the part of legal experts. More to the point is the fundamental consideration that the basic purpose of self-defense is to ward off armed attack. There are no compelling reasons to rule out the right of a State to exercise self-defense in the face of the clear ability of a number of armed groups to conduct an armed attack that is comparable in scale and effects to attacks conducted directly or indirectly by States.[13]

AFGHANISTAN 33, 40 (Rober Beeres et al. eds., 2012) and Ducheine & Pouw, *supra* note 10, at 67–69.

12. *See* Ducheine & Pouw, *Legitimizing the Use of Force*, *supra* note 11, at 39.

13. The UN Security Council implicitly recognized this possibility in Resolutions 1368 and 1373 by referring to "the inherent right of self-defense." S.C. Res. 1368, pmbl., U.N. Doc. S/RES/1368 (Sept. 12, 2001); S.C. Res. 1373, para. 4, U.N. Doc. S/RES/1373 (Sept. 28, 2001). Following the 9-11 attacks, NATO and the Organization of American States also recognized that attacks by armed groups could give rise to the right of self-defense. *See* Press Release, North Atlantic Treaty Organization, Statement by the North Atlantic Council (Sept. 12, 2001), *available at* http://www.nato.int/docu/pr/2001/p01-124e.htm; Terrorist Threat to the Americas, Res. 1, Twenty-Fourth Meeting of Consultation of Ministers of Foreign Affairs Acting as Organ of Consultation In Application of the Inter-American Treaty of Reciprocal Assistance, OEA/Ser.F/II.24, RC.24/RES.1/01 (Sept. 21, 2001). The ICJ cast doubt on whether an armed attack conducted by an armed group gave rise to the right of self-defense in the absence of State support in its advisory opinion on the *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 2004 I.C.J. 136, 194 (July 9), and its judgment in *Armed Activities on the Territory of the Congo* (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 116 (Dec. 19). The latter decision was met, however, with vigorous criticism by a number of the judges in their separate opinions. A large number of recognized authorities believe an armed attack being conducted by a non-State entity in the absence of State control can give rise to the right of self-defense. *See, e.g.*, DINSTEIN, *supra* note 5, at 227–30; Michael N. Schmitt, *Responding to Transnational Terrorism under the* Jus ad Bellum, *in* INTERNATIONAL LAW AND ARMED CONFLICT: EXPLORING THE FAULTLINES—ESSAYS IN HONOUR OF YORAM DINSTEIN 157 (Michael N. Schmitt & Jelena Pejic eds., 2007). The views of one of the present authors

3. Requirements Related to the Security Council

In addition to the requirement of an armed attack, the Charter stipulates that actions of self-defense may only be carried out until such time as the Security Council has undertaken the measures necessary to restore international peace and security. This is the concrete manifestation of the primary purpose for including the right of self-defense in the Charter. It was not to definitively codify—much less invent—this long existing right, but rather to integrate it into the Charter system of collective security and provide a secure legal basis for collective self-defense treaty arrangements. The Council exercises primacy in the realm of the maintenance and restoration of international peace and security as reflected in, *inter alia*, Article 51 of the Charter.

Additionally, a procedural requirement to report measures of self-defense to the Council at the earliest possible opportunity is incorporated into this provision. It should be stressed that the requirement of reporting to the Council does not translate into a requirement to obtain prior authorization to exercise the right. Likewise, not just any action undertaken by the Security Council has the effect of terminating the right of a State to exercise self-defense. Only measures that are necessary (implying effectiveness when read in conjunction with Article 1(1) of the Charter) to restore peace and security and that are explicitly intended to terminate the exercise of the right by a State will have such effect.[14] It is the Council that decides whether the measures it has taken are sufficient to remove the necessity of exercising self-defense, but in the absence of an explicit intention expressed by the Council, for example, in the form of a cease and desist order, there is

---

are set out in more detail in Terry D. Gill, *The Temporal Dimension of Self-Defense Anticipation, Pre-emption, Prevention and Immediacy*, *in id.* at 113, 118. The essential reason giving rise to the possibility of responding in self-defense to an armed attack conducted by a non-State entity operating from the territory of a host State lies in the duty of States under international law to prevent their territory from being used to carry out actions that violate the rights of other States, including, in particular, the right to territorial inviolability and integrity. This duty of due diligence is part of customary law and was recognized, *inter alia*, in the *Island of Palmas* arbitral award (Island of Palmas (Neth. v. U.S.), 2 R.I.I.A. 829 (Perm. Ct. Arb. 1928)) and by the ICJ in the *Corfu Channel* judgment. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, 22–23 (Apr. 9).

14. *See* Gill, *supra* note 4, at 195–96.

no presumption that measures taken by the Council have the effect of terminating the right of self-defense in and of themselves.[15]

C. Conditions Laid Out in Customary International Law

Because self-defense has, as we have seen, a dual-legal basis, it is clear that it must conform to the conditions laid out in both sources. Under customary law, any exercise of self-defense must be carried out in a manner consistent with the principles of necessity, proportionality and immediacy. These were formulated in the diplomatic exchanges following the well-known 1837 *Caroline* incident, which has been described by Jennings as the *locus classicus* of the law of self-defense.[16] There is no mention of these principles in Article 51 for the simple reason that, as previously noted, it was not intended to comprehensively codify the law relating to self-defense. These criteria are of a customary nature and complement the requirements flowing from the Charter.

15. The primacy of the Council is evident from the text of Article 51, which, when read in conjunction with Articles 24 and 1, sets out the Council's authority in the maintenance of peace and the fundamental purpose of the Charter—the maintenance and restoration of international peace and security through effective collective measures. *See* DINSTEIN, *supra* note 5, at 238–39; Waldock, *supra* note 5, at 495–96; ROSALYN HIGGINS, PROBLEMS AND PROCESS: INTERNATIONAL LAW AND HOW WE USE IT 239–40 (1994). In Security Council Resolution 598, the Council ordered both parties to the Iran-Iraq War to stand down. S.C. Res. 598, ¶ 1, U.N. Doc. S/RES/598 (July 20, 1987). In contrast, in Resolution 1373, *supra* note 13, the Council adopted a whole range of mandatory measures not involving the use of force aimed at combating international terrorism, while at the same time affirming the right of self-defense in connection with the armed attack of 9-11. In the Desert Shield/Desert Storm operations of 1990–91, the right of self-defense continued to operate alongside—and was ultimately subsumed into—the collective measures adopted by the Security Council in Resolutions 660–678 (1990).

16. R.Y. Jennings, *The Caroline and McLeod Cases*, 32 AMERICAN JOURNAL OF INTERNATIONAL LAW 82, 92 (1938). For a discussion of the principles of necessity and proportionality and their distinct meanings in the *ius ad bellum*, as opposed to their meaning in the context of other branches of the law, such as the law of armed conflict, see, e.g., JUDITH GARDAM, NECESSITY, PROPORTIONALITY AND THE USE OF FORCE BY STATES 10 (2004). *See also* DINSTEIN, *supra* note 5, at 231–33; OSCAR SCHACHTER, INTERNATIONAL LAW IN THEORY AND PRACTICE 152–55 (1991).

1. Necessity

Necessity in the context of self-defense requires the existence of an armed attack that is ongoing or imminent and for which no other feasible alternative response exists.

An attack can be a single large-scale attack or a series of related small-scale attacks from the same source, which together form a single attack. It can also be a manifestly imminent attack in the proximate future, a point to which we will return below.

Alternatives can include measures short of self-defense when these are available. In the context of attacks by non-State actors, this includes exercising law enforcement measures whenever this is feasible and provides an adequate response. This is of particular importance with regard to a possible cyber armed attack conducted by a non-State actor with a greater or lesser degree of organization operating from a territory where the government is both willing and able to conduct or permit an effective law enforcement response. When the Security Council implements effective collective measures, the right of self-defense can be complemented by such measures, subsumed into them, or the right can be terminated when the Council so directs. A clearly expressed willingness to cease an attack, including compliance with ceasefire/withdrawal orders by the Security Council, coupled with adequate measures to ensure non-repetition and a willingness to conclude a comprehensive settlement of outstanding issues by peaceful means can also constitute an alternative to continued exercise of the right of self-defense.[17]

It should be emphasized that seeking or obtaining prior consent does not in general or as a matter of law form part of the principle of necessity. If an attack is ongoing (or as we will argue more extensively below is imminent), there is no requirement to obtain prior consent to exercise the right of self-defense. If an attack has not yet materialized, there is no necessity and, therefore, no right to exercise self-defense.

When armed attacks are being conducted by a non-State actor operating from one State's territory against another State and the non-State actor

17. Law enforcement measures are specifically and uniquely responses to attacks conducted by non-State groups. They can provide a feasible alternative in situations where the State from which the attack originated has control over its territory and is willing to undertake effective law means to address the threat. This would be the logical alternative to the use of trans-boundary armed force in self-defense. See the views of one of the present authors in Ducheine & Pouw, *Legitimizing the Use of Force, supra* note 11, at 64–65.

is neither under the control of the territorial State nor acting with its complicity, remedial action should be taken by the State where the non-State actor is located. This may take the form of adequate law enforcement measures or a proportionate recourse to armed force (either unilateral force or force used with the consent of the territorial State). If the territorial State consented, that consent would serve as a legal basis, in addition to or in place of self-defense, for the taking of action by the target State to forestall the attack.

2. Proportionality

Proportionality in the context of self-defense refers to the requirement that measures of self-defense must not exceed those required under the circumstances to repel the attack and prevent further attacks from the same source in the proximate future and that they must be roughly commensurate to the scale and aims of the overall attack. Hence, the scale and nature of the attack will determine what is required to repel or, if necessary, overcome it and prevent a continuation. A proportionate response to a single isolated armed attack would be measures to ward off the attack and prevent any direct and immediate threat of repetition. For example, a warship targeted by an anti-ship missile fired from a shore-based installation could take measures to ward off the attack and neutralize the immediate source of the attack. A more substantial, but still relatively limited, attack against a State's territory or military forces abroad would permit a response that warded off the immediate attack and forestalled repetition in the proximate future. A proportionate response to a full-scale armed attack, e.g., an invasion or large-scale offensive strike, would be a defensive war aimed at defeating the attacking party and removing the threat of further aggression.

Proportionality requires neither exact mathematical equivalency nor does it dictate the modality of exercising self-defense. If a digital attack rises above the threshold of armed attack, the response may be to employ cyber weapons or kinetic force or a combination of the two to neutralize the attack, as long as the response did not exceed that required to repel the attack. Proportionality does not permit measures that would needlessly prolong or exacerbate the conflict.[18]

18. See the authorities cited *supra* note 16. With regard to proportionality and the "accumulation of events" theory, discussed *supra* note 10 and accompanying text, see the report by Roberto Ago in his capacity as Special Rapporteur to the International Law Commission. Robert Ago, *Addendum to the Eighth Report on State Responsibility,* [1980] 2

3. Immediacy

Immediacy as a separate criterion for the exercise of self-defense refers to the requirement that self-defense measures, after taking the relevant circumstances into account, must not be unduly delayed. This requirement relates to the distinction between self-defense, which is a recognized legal basis for the use of force, and armed reprisal, which is unlawful under contemporary international law. Once an armed attack has occurred and the source of the attack determined, the defending State must proceed with its defensive measures as soon as it is capable of mounting a defense. This does not mean, however, that a response must necessarily be instantaneous to be lawful. A State will need to explore whether there are feasible alternatives to the use of force in instances when it is not readily apparent that there are none. It may need to deploy forces to the source of the attack, mobilize forces that are not in a state of instant readiness, consult with allies and receive assistance in order to be able to respond, identify the attacker when this is not readily evident. The latter requirement is particularly relevant in the cyber context, as well as in certain other types and modes of attack. The important point is that self-defense is exercised within a reasonable timeframe in response to an ongoing attack or, as we will demonstrate below, a clear threat of attack in the proximate future. It is not a punitive measure to be undertaken long after the attack has been carried out. A State does not, however, forfeit its right of self-defense because it is incapable of instantly responding or is uncertain of who is responsible for the attack or from where the attack originated.[19]

4. Evidence

In addition to the necessity, proportionality and immediacy principles, there must be credible evidence as to the identity of the attacking party and the source of the armed attack before measures in self-defense can be taken. International law does not have a comprehensive set of universally recognized evidentiary standards to apply in determining whether a defensive

---

YEARBOOK OF THE INTERNATIONAL LAW COMMISSION pt. 1, 13, 69–70, U.N. Doc. A/CN.4/318/ADD.5-7 (1980).

19. With respect to immediacy as a general criterion for the exercise of self-defense, see Gill, *supra* note 13, at 151–54.

response is permitted in situations where the identity and source of the attack is not readily apparent.[20]

In traditional attacks involving the armed forces of one State attacking the forces or territory of another State, the identity of the attacking party will usually be readily apparent. There was clearly no doubt of the identity of the attacking State at Pearl Harbor in 1941 and the invading State in Kuwait in 1990. However, in situations where an armed group acts as either a proxy of a State or on its own to carry out an armed attack or series of attacks, it may be less than clear who or what is behind the attack, particularly when the author of the attack denies involvement. The case law of the International Court of Justice in rejecting "suggestive" and "highly suggestive" evidence seems to point to a stringent level of proof, but there is less than full agreement within the Court and the international community at large as to the accuracy of the standard it employs.[21]

The requirements for evidence in the criminal justice system of most States and before international criminal tribunals would hardly be feasible or realistic when acting in self-defense.[22] Nevertheless, there must be reasonably credible and convincing evidence of involvement before a State can take measures in self-defense against a particular State or entity such as an armed group suspected of perpetrating an armed attack in instances where the identity of the attacker is not readily apparent.

D. The Temporal Dimension: Anticipatory Self-Defense

We will now turn to the question whether international law permits the exercise of measures of self-defense in response to an imminent or potential armed attack.

Before presenting our views, it is necessary to clarify some terminology. In this article, the term "anticipatory self-defense" denotes defensive

---

20. The ICJ employed a stringent standard that rejected "suggestive" and "highly suggestive" evidence of Iranian involvement in attacks on international shipping in the Persian Gulf. Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶¶ 59, 71 (Nov. 6). This and other aspects of the judgment were vigorously criticized by a number of judges in their individual opinions. *See id.*, ¶¶ 30–39 (separate opinion of Judge Higgins); *id.*, ¶¶ 21–30 (separate opinion of Judge Kooijmans); *id.*, ¶¶ 33–46 (separate opinion of Judge Buergenthal); *id.*, ¶¶ 33–40 (separate opinion of Judge Owada).

21. *Id.*

22. There is no generally accepted "law of evidence" in international law. Standards differ between criminal tribunals and other international decision making bodies, e.g., arbitrations.

measures undertaken in response to a manifest and unequivocal threat of attack in the proximate future. The term "*preemptive* self-defense" is synonymous. The term "*preventive* self-defense" signifies a defensive response to an inchoate or potential threat of attack at some indeterminate point in the future.

There is at present no universal consensus on the legality of either of these modes of exercising self-defense in advance of an actual attack.[23] It is nevertheless fair to say that the former mode (anticipatory or preemptive self-defense) enjoys widespread support among a significant number of States and in juridical opinion, while preventive self-defense is much more controversial.[24]

In our view, anticipatory self-defense has long been recognized in customary international law. The existence of an anticipatory element in self-defense is, moreover, part of the essence of the right of self-defense in that forestalling continued attack, in addition to responding to an ongoing attack, is part of the necessity and proportionality criteria that are integral elements of self-defense. In that sense, self-defense is both forward looking, by securing the defending State from future attack, as well as reactive, by repelling an attack in progress. Any other rendition would leave a defending State in an untenable and highly vulnerable position; one which, would put it in an unequal position *vis-à-vis* the attacking party. This neither makes sense nor does justice to the purpose underlying the right of self-defense.

The recognition of this anticipatory element can be traced back to the previously mentioned *Caroline* incident. In the diplomatic correspondence following that incident, the general conditions for the exercise of self-defense, including its temporal dimension were set out. These were, in nineteenth century prose, "a necessity of self-defense, instant, overwhelming and leaving no choice of means and no moment for deliberation."[25]

---

23. For a clear discussion of the controversy concerning the temporal aspect of self-defense, see KINGA T. SZABO, ANTICIPATORY ACTION IN SELF-DEFENCE 6–8 (2011).

24. On the legality of preventive self-defense, see High-Level Panel on Threats, Challenges and Change, *A More Secure World: Our Responsibility*, U.N. Doc. A/59/565 (Dec. 2, 2004); U.N. Secretary-General, *In Larger Freedom: Towards Development, Security and Human Rights for All*, U.N Doc. A/59/2005, 59th Sess., (Mar. 21, 2005).

25. On the *Caroline* incident, see MICHAEL BYERS, WAR LAW 53–54 (2003); BROWNLIE, *supra*, note 5, at 42–43; DINSTEIN, *supra* note 5, at 197–98; THOMAS FRANCK, RECOURSE TO FORCE 97–98 (2002). The most authoritative article on the *Caroline* incident remains without doubt that by R.Y. Jennings, *supra* note 16. The primary source for information on the *Caroline* incident and the exchange of correspondence between Webster

This formulation of the general conditions for the exercise of anticipatory self-defense is widely regarded as authoritative and has had a lasting influence, although not without a certain degree of divergence of opinion as to how literally the wording used should be taken. There is also disagreement among authorities and States as to whether it is a valid precedent and, even if it is, whether anticipatory self-defense is still lawful under the UN Charter regime.

This is not the place to delve into the historical value of the *Caroline* incident in depth, but two points deserve attention. First, it is sometimes argued that since *Caroline* took place in an era and under a legal regime in which war was lawful, it is of little relevance under the present day Charter legal regime in which not only war, but the use of force are prohibited, barring strict exceptions. This critique, it is submitted, is incomplete and, therefore, incorrect. While it is true that recourse to war was lawful in the nineteenth century legal order, the attack on the *Caroline* did not constitute a war. The use of trans-boundary force below the threshold of war (often referred to as "measures short of war") required a legal justification in the pre-Charter legal order. Acts involving a use of force that fell outside the legal context of a "state of war," either declared or factual, such as various types of intervention, hot pursuit of armed bands over a frontier, pacific blockade and armed reprisal, were then regulated in international law—as they are now—although many of the legal rules relating to these uses of force were substantially different in the nineteenth century than they are under the Charter. Nevertheless, it is erroneous to conclude that because war was lawful in the international law of the nineteenth century, that legal justifications for using force were irrelevant.

Nor is it convincing to argue that since the British action was directed against a non-State entity (groups of American nationals acting without U.S. sponsorship who sympathized with the rebellion taking place in British North America), it falls under the rubric of "state of necessity" rather than self-defense. The diplomatic correspondence referred to self-defense as the justification, not necessity, and it was viewed as such by both parties to the dispute. More recently, the decisions of the Nuremburg and Tokyo tribunals held following the conclusion of World War II cited the *Caroline* incident in analyzing claims of self-defense by German and Japanese defendants. Moreover, the critique reflects a position that self-defense can

---

and Fox is found in 29 BRITISH AND FOREIGN STATE PAPERS 1129, 1137–38 (1840–41), and between Webster and Ashburton, found in 30 BRITISH AND FOREIGN STATE PAPERS 195, 195–96 (1841-42).

pertain only to attacks conducted by a State or by an armed group under the control of a State: that interpretation was not the law then, nor does it, as discussed above, reflect current practice. Finally, notwithstanding significant divergences between the nineteenth century law on the use of forcible measures short of war and the contemporary legal order, the principles of necessity, proportionality and immediacy, which were agreed to by both States in the *Caroline* incident, have not undergone significant transformation and are still of undisputed relevance today in the context of self-defense, although the circumstances in which they are applied may have altered significantly in some situations.[26]

Second, as regards the precedential value of the *Caroline* formula, it is undisputed that the references made to it in the Nuremburg and Tokyo trials reflect a conviction that it represented customary international law at the very time the Charter was drafted and entering into force.[27] Without

---

26. On the nineteenth century law relating to the use of force short of war, see STEPHEN C. NEFF, WAR AND THE LAW OF NATIONS: A GENERAL HISTORY 156 (2005) and SZABO, *supra* note 23, at 69–77. The right of self-defense in the nineteenth century was related to both the natural law concept of "imperfect war" and the broader notion of self-preservation. Szabo rightly points out that the nineteenth century notion of self-defense referred to in the *Caroline* incident included an intrinsic anticipatory element, therefore, there was no separate category of anticipatory self-defense at that time. *Id.* at 75. The opinions of commentators as to the relevance of customary law and pre-Charter precedents, such as the *Caroline* incident, can be roughly divided into two schools. One, exemplified by such writers as BROWNLIE, *supra* note 5, at 25; DINSTEIN, *supra* note 5, at 188–89; and CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 86–88 (2000), largely or wholly discount the relevance of pre-Charter practice relating to self-defense because it took place in an era when recourse to force was not unlawful. Others, such as BOWETT, *supra* note 5, at 269; FRANCK, *supra* note 25, at 45; and Waldock, *supra* note 5, at 455, take a wider view and consider pre-Charter practice as relevant.

27. For the Nuremburg judgment on the relevance of the *Caroline* criteria to the German plea of preventive self-defense in connection with its invasion of Norway, see 22 TRIAL OF THE MAJOR GERMAN WAR CRIMINALS BEFORE THE INTERNATIONAL MILITARY TRIBUNAL 448–50 (1948), *available at* http://www.loc.gov/rr/frd/ Military_Law/pdf/NT_Vol-XXII.pdf. For the assessment of the declaration of war by the Netherlands on Japan, see JUDGMENT OF THE INTERNATIONAL MILITARY TRIBUNAL FOR THE FAR EAST 379–84 (1946). The Japanese did not commence operations directly against the Netherlands East Indies until January 11, 1942, over a month after the attack on Pearl Harbor, because they first had to deal with American and British forces in the Philippines, Hong Kong and Malaya. The Tribunal pointed out that it was evident from the scale of the Japanese offensive across the Pacific and Southeast Asia that the Netherlands East Indies were going to be attacked as soon as it was practicable, and that, in fact, plans to that effect had been made prior to the attack on Pearl Harbor. Obviously, the plans were not made public so the Netherlands was unaware of them at the time. Nevertheless, the

firm evidence that customary law has evolved in a different direction since then, there is no reason to assume the present legal regime no longer allows for some degree of anticipatory self-defense.[28] Stated differently, if international law relating to the exercise of self-defense in the period in which the Charter was adopted contained an anticipatory element, then the assumption would be that it continues to exist, unless it could be conclusively shown that it had been subsequently altered, with the burden of proof resting on those who hold the law has changed.

Certainly, more is required than simply stating that the wording of Article 51 of the UN Charter, with its phrase "if an armed attack occurs," categorically rules out anticipatory self-defense, since the wording itself sheds no light on either what constitutes an armed attack or when it can be said to have occurred. If one assumes an armed attack only occurs when a particular use of force physically passes an international boundary, there would, indeed, be no scope for anticipatory self-defense. However, this is not the only, nor necessarily the most convincing, interpretation of the meaning of the "occurrence" of an armed attack.

In both the nineteenth century and at the time the Charter was adopted, armed attack was considered to include clear and manifest preparations, even the intention to attack in the proximate future, when their existence was supported by clear evidence. The Nuremburg Tribunal rejected the German defendants' plea of self-defense as justifying the invasion of Norway in April 1940, not because it rejected the possibility of preemption as such, but because the evidence clearly pointed to motives other than self-defense. The Tribunal held that the basis for self-defense was lacking even though the Allies had contemplated a possible intervention in northern Norway to come to the assistance of Finland, which was being attacked by the Soviet Union at the time, and to interdict the shipment of Swedish iron ore to Germany, because Germans were not aware of these contingency plans when they carried out the invasion.

Dutch declaration of war enabled the formation of a joint defensive effort by U.S., British, Australian and Dutch forces in Southeast Asia. The Tribunal deemed it to be defensive in character in accordance with the *Caroline* criteria in response to an aggressive war launched by Japan. For a chronology of the Japanese offensive against the Netherlands East Indies and the formation of the joint defense by the Allies, which culminated in the defeat of Dutch, U.S., Australian and UK naval forces in the Battle of the Java Sea and the completion of the conquest of the Netherlands East Indies by March 1942*,* see RICHARD E. DUPUY & TREVOR N. DUPUY, THE ENCYCLOPEDIA OF MILITARY HISTORY 1132, 1138 (2d ed. 1986).

28. See sources cited *supra* note 7. *See also* SZABO, *supra* note 23, at 125.

Likewise, the Tokyo Tribunal held the declaration of war by the Netherlands against Japan immediately after the attack on Pearl Harbor, which occurred well before the Japanese commenced military operations against the Dutch East Indies, did not give rise to a right of self-defense by Japan. It so held because it was evident that the scale of the Japanese offensive throughout the Pacific and East Asia was so comprehensive as to include the intention to capture the Dutch colony once it had been reached, after overcoming resistance elsewhere, in order to secure the valuable natural resources located there that were vital to the Japanese war effort. In short, an armed attack was considered to have "occurred" at a time it was evident an attack was going to take place in the near future, even though this was well before any forces ever crossed the frontier, or even concrete measures—as opposed to preparations—had been taken to initiate an attack against Dutch-administered territory. That is the definition of anticipatory self-defense as it comes to current international law from the *Caroline* formula; it is essentially taking action within the last feasible "window of opportunity" once the intention and capability to mount an attack have become clear.[29]

Since the adoption of the Charter, there have been references by States to the existence of the right of anticipatory self-defense on various occasions and in various contexts. While certain invocations have not met with general acceptance, others have. It is particularly noteworthy that no international court or tribunal, nor the Security Council, has ever ruled out recourse to anticipatory self-defense within the general confines of the *Caroline* formula as a matter of law. For that matter, the General Assembly has never made any such pronouncement: neither in the well-known 1970

29. The clear distinction between self-defense, including warding off the manifest danger of impending attack, and preventive self-defense (which is a contradiction in terms since it is based on the mere belief that an attack *might possibly* occur at some indeterminate point in the future and *might possibly* be directed against an indeterminate target State) is the existence of a necessity to act when no feasible sufficient alternatives to defensive force are available. The principles of necessity and immediacy are what set self-defense apart from other uses of force. In this context, necessity and immediacy do not necessarily translate into a specific time period in which a State faced with the clear and present danger of an impending attack must act, but they must be seen in context and are tied to the lack of feasible alternatives. While, in general, the longer the period before an attack is launched the less likely it is that there will be no feasible alternatives, this is not always the case as is demonstrated in, *inter alia*, the Dutch declaration of war against Japan, where the intention and capability to conduct an attack were clear and convincing. For the concept of the "last window of opportunity," see, e.g., TALLINN MANUAL*, supra* note 3, rules 14 & 15 with commentary.

"Friendly Relations" declaration, which restated and interpreted the basic principles of the Charter, nor in the 1974 "Definition of Aggression" declaration, which serves as the basis for the definition of the crime of aggression in the Rome Statute of the International Criminal Court.[30]

In addition, the well-respected *Institut de Droit International* and the High-Level Panel on Threats, Challenges and Change, which advised the UN Secretary-General in 2004, have taken the position that anticipatory self-defense within the parameters of the *Caroline* criteria is permissible under contemporary international law.[31]

In conclusion, there is ample evidence that the right of self-defense contained an anticipatory element at the time the Charter was adopted and that it continues to do so now. In the absence of conclusive evidence that the law has been altered since the Charter entered into force, there is no reason to assume that anticipatory self-defense when exercised within the confines of the *Caroline* criteria has become unlawful.

III. ANTICIPATORY SELF-DEFENSE AND A CYBER ARMED ATTACK

A. Cyber Armed Attack: Likelihood and Possible Modalities

Having set out the applicable legal framework in the previous section, we will now proceed to apply it to a cyber attack that rises to the level of an armed attack in a legal sense. Two things should be pointed out at the outset. First, the term "cyber attack," as it is widely used in the media and by members of the cyber community, is not necessarily synonymous with the notion of armed attack under the international law of self-defense. In the vast majority of cases, incidents referred to as a "cyber attack" have not constituted a use of force, much less one rising to the threshold of an armed attack. The denial-of-service "attack" on Estonia in 2007, which resulted in a few hours of disruption and inconvenience, and numerous examples of cyber break-ins, espionage, sabotage and theft of data and intel-

30. Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, G.A. Res. 2625 (XXV), U.N. Doc. A/8082 (Oct. 24, 1970); Definition of Aggression, G.A. Res. 3314 (XXIX), U.N. Doc. A/RES/3314 (Dec. 14, 1974), Rome Statute of the International Criminal Court, July 17, 1998, 2187 U.N.T.S. 90.

31. High-Level Panel, *supra* note 24, ¶¶ 188, 54 (Dec. 2, 2004); W. Michael Reisman, Report, Tenth Commission, *Present Problems of the Use of Armed Force in International Law*, 72 ANNUAIRE DE L'INSTITUT DE DROIT INTERNATIONAL 237 (2007).

lectual property constitute neither a use of force nor an armed attack.[32] Indeed, it is very probable that no breach of cyber security loosely referred to as a "cyber attack" has to date reached the level of an armed attack in a legal sense.[33] That is our position, since, to our knowledge, none has been so regarded in State practice and none has resulted in death, injury or significant long-term material damage to critical infrastructure on which the functioning of a State depends. The only example that might be viewed otherwise is Operation Olympic Games,[34] or Myrtus as it was also known,[35] the Stuxnet cyber attack on the Iranian nuclear weapons program during the period 2008–10 that reportedly caused a measure of physical damage to the centrifuges engaged in the enhancement of nuclear material.[36] While this may be an arguable example of an armed attack, in our view it is better treated as an example of mere sabotage not amounting to an armed attack, since it neither resulted in physical injury or death to persons, and the damage had no wider, long-term or serious secondary effects beyond apparently delaying the progress of the Iranian nuclear program for several months. This could hardly be deemed to constitute critical infrastructure[37] damage seriously impairing the functioning of the State or the stability of Iranian society.

1. Stand-alone Cyber Attack

Second, while the possibility of a stand-alone cyber attack, that is, one not occurring in conjunction with an attack employing traditional kinetic force, rising to the level of an armed attack cannot be ruled out, it is not in our

32. For an overview, see, e.g., Thomas Rid, *Cyber War Will Not Take Place*, 35 JOURNAL OF STRATEGIC STUDIES 1, 5–32 (2012) *reprinted in* CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 2, ch. 4.

33. *Id.* at 75.

34. DAVID SANGER, CONFRONT, & CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER (2012).

35. Rid, *supra* note 32, at 85.

36. *See, e.g.*, David P. Fidler, *Was Stuxnet an Act of War? Decoding a Cyberattack*, 9 IEEE SECURITY AND PRIVACY MAGAZINE 4, 56–59 (2011); Michael.J. Gross, *A Declaration of Cyber-War*, VANITY FAIR, Apr. 2011, at 152, *available at* http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.print.

37. Iran is not dependent on nuclear energy. According to the CIA World Factbook, Iran's electricity consumption is generated from fossil fuels (86.1%) and hydroelectric plants (13.7%). CENTRAL INTELLIGENCE AGENCY, THE WORLD FACTBOOK, https://www.cia.gov/library/publications/the-world-factbook/geos/ir.html (last visited July 30, 2012)

view the most likely form of attack.[38] The majority of potential cyber attacks are not likely to cause physical casualties or significantly degrade a State's critical infrastructure for a significant period of time, although undeniably some could have that capability. The exaggerations of so-called "cyber doom scenarios" have been compared to air-power theorists prior to and during World War II, who took the position that strategic bombing on its own could bring about the complete destruction of a State and its social fabric. They have also been attributed to the psychological aftermath of the 9-11 attack and to longstanding inchoate fears of technology and its potential effects that predate the digital age, but which have gained new adherents as the result of the dependency of contemporary society on digital systems.[39]

Be that as it may, no cyber attack on its own has to date constituted an armed attack. While the possibility of a cyber armed attack can and should not as a matter of prudence be ruled out, it should not be confused with real cyber security threats that do take place on an ongoing and regular basis in the form of cyber espionage, cyber sabotage and cyber criminal activity aimed at both public and private computer systems. However, as serious as these threats may be to a State's national and economic security, they do not constitute armed attacks that would justify the use of force in self-defense.

Only cyber attacks having direct secondary effects resulting in physical casualties, substantial physical damage, or such substantial and long-term damage to critical infrastructure that the carrying out of a State's essential functions or its social and political stability are seriously impaired should, we submit, be treated as armed attack in the sense of the law relating to the exercise of self-defense. While an attack of this magnitude is feasible and

38. In general, a cyber sabotage attack against the supervisory control and data acquisition (SCADA) system of chemical plants, could result in damage, e.g., the leakage of poisonous gasses. There is a potential for a more serious incident when plants are situated closely to densely populated areas, as is the case in the Netherlands where Royal Dutch Shell's chemical installations are close to the port and city of Rotterdam. According to Rose Tsang, however, "it is unlikely such an [intentional] attack [by an individual or small group of individuals] would result in a wide-scale failure of the critical infrastructure." Rose Tsang, *Cyberthreats, Vulnerabilities and Attacks on SCADA Networks* 21 (University of California, Goldman School of Public Policy, Working Paper, 2009).

39. *See* Sean Lawson, *Beyond Cyber Doom—Cyber Attack Scenarios and the Evidence of History*, 10 JOURNAL OF INFORMATION TECHNOLOGY & POLITICS 1, 4 (2013), *reprinted in* CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 2, ch. 13.

cannot be wholly discounted, the unlikelihood of it occurring should be kept in mind.[40]

2. Combined Attack: Cyber Operations and Kinetic Attack

If stand-alone cyber armed attacks are probably less likely to occur than is sometimes conjectured, what other options are there? In our view, the most likely is an armed attack involving cyber operations carried out in conjunction with a traditional use of kinetic armed force. There are two known instances where this has occurred.

One was during the armed conflict between Russia and Georgia in August 2008, when Georgia initiated armed action against South Ossetian separatists and Russia intervened militarily, forcing the Georgian armed forces to withdraw.[41] For purposes of this article, we are not concerned with the legality of the use of force by either side to the conflict, rather our focus is on the cyber operations conducted by Russian State agencies and/or supportive patriotic hackers (there was no clear evidence as to who was responsible). These were limited in effect and duration and did not constitute an armed attack. If, however, they had gone beyond mere defacing of government websites and inconveniencing the public and certain public bodies, to, e.g., support military operations by degrading or neutralizing weapons and military communications systems, in that case they would have constituted armed attacks. If used in such a manner, it would have been part of an overall armed attack involving the use of traditional military force that included the employment of cyber techniques as an adjunct to, or preparation for, the kinetic attack.

That is what apparently occurred in Operation Orchard, when Israel carried out an airstrike against the Al-Kibar nuclear facility in northern Syria in September 2007.[42] The airstrike was seemingly accompanied by the

40. The authors share the view expressed by Tsang, *supra* note 38.

41. *See* ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS (2010); Keir Giles, *"Information Troops"—a Russian Cyber Command?*, *in* 3RD INTERNATIONAL CONFERENCE ON CYBER CONFLICT 45, 46 (Christian Czosseck, Enn Tyugu & Thomas Wingfield eds., 2011).

42. Andrew Garwood-Gowers, *Israel's Airstrike on Syria's Al-Kibar Facility: a Test Case for the Doctrine of Pre-Emptive Self-Defence?*, 16 JOURNAL OF CONFLICT AND SECURITY LAW 263 (2011). Daveed Gartenstein-Ross & Joshua D. Goodman, *The Attack on Syria's al-Kibar Nuclear Facility*, INFOCUS QUARTERLY, Spring 2009, *available at* http://www.jewishpolicycenter.org/826/the-attack-on-syrias-al-kibar-nuclear-facility; *Isra-*

use of cyber electronic warfare that reportedly neutralized the Syrian air defense system and enabled the airstrike to be carried out successfully.[43] Again, without addressing the question of whether this act was a lawful exercise of self-defense, it is a clear illustration of an armed attack in which cyber capabilities were used alongside traditional kinetic armed force as a means of "preparing the battlefield," thereby creating favorable circumstances for the overall success of the operation. This type of cyber operation will almost inevitably become more prevalent as more States obtain the capacity to effectively utilize cyber as an adjunct to traditional kinetic force and integrate it into their operational doctrine and practice.[44] Armed forces will start—as some have already started—to ensure a coherent integration of cyber capabilities across the spectrum of military operations.[45]

In our view, the combination of cyber and kinetic attacks is a far more likely scenario than a stand-alone cyber armed attack. There are several reasons why a stand-alone cyber attack rising to the level of an armed attack is considerably less likely than a combined attack.

On the one hand, if the attack were part of a large-scale offensive comprising a concerted series of attacks, it is unlikely that the attacking State would rely solely on one particular form of attack. A stand-alone "cyber Pearl Harbor" scenario is, therefore, highly unlikely, since an attack on that scale as the opening move in a full-scale war would inevitably trigger a large-scale kinetic response. Thus, it would make little sense to limit the initial attack to a cyber attack. If a State, having decided to go to war, employed cyber in such a large-scale attack that it amounted to the com-

---

el Admits Air Strike on Syria, BBC NEWS (Oct. 2, 2007, 17:12 GMT), http://news.bbc.co.uk/2/hi/7024287.stm.

43. David A. Fulghum & Douglas Barrie, *Israel Used Electronic Attack in Air Strike Against Syrian Mystery Target*, AVIATION WEEK, Oct. 8, 2007, at 28, *available at* http://www.freerepublic.com/focus/f-news/1908050/posts.

44. For national military doctrines, see ENEKEN TIKK, FRAMEWORKS FOR INTERNATIONAL CYBER SECURITY, NATIONAL CYBER SECURITY POLICIES AND STRATEGIES (2011).

45. *See* PRIME MINISTER DAVID CAMERON, SECURING BRITAIN IN AN AGE OF UNCERTAINTY: THE STRATEGIC DEFENCE AND SECURITY REVIEW 27 (2010), *available at* http://www.official-documents.gov.uk/document/cm79/7948/7948.asp ("Future conflict will see cyber operations conducted in parallel with more conventional actions in the maritime, land and air environments.").

mencement of the war, it would most likely be in conjunction with other means of attack to ensure the maximum effect was realized.[46]

If, on the other hand, a cyber operation was employed against a single discrete target, it would more than likely take the form of either an act of cyber espionage or sabotage below the threshold of armed attack, as in the Stuxnet scenario, or be used in support of a kinetic attack if the intention was to destroy the target, as was the case with the 2007 Israeli airstrike on the Al-Kibar nuclear facility. A stand-alone cyber attack that actually caused a significant degree of physical damage to an installation or resulted in human casualties, thereby constituting an armed attack, would not necessarily destroy a target.

Moreover, using cyber alone as a means of inflicting significant physical damage or substantial loss of life would almost certainly increase the risk of miscalculation and escalation, because of the degree of unpredictability and relative anonymity of a cyber attack. Additionally, the probable psychological impact of an attack on one specific target would seem senseless for political and military purposes or in legal terms, assuming these mattered to the actor involved. A more likely course of action in a cyber operation intended to degrade a particular target would be to stay below the threshold of an armed attack, thereby allowing an actor that wished to degrade a particular target to do so with much less risk of a forcible response and to maintain denial of direct involvement, as was the case with Stuxnet. In sum, if the desired end state was destruction of a target, cyber would not be the method of attack most guaranteed to succeed, while if the objective was merely to obtain information or degrade a target without destroying it and risking escalation, it would not require a cyber attack that rose to the level of an armed attack.

3. Rational Actor

Of course, this discussion has assumed the actor is reasonabe and acts with rational motives and objectives, whether they are legal or illegal. The proverbial "genie in the bottle" is, of course, a large-scale act of cyber terrorism that has the potential effect of causing massive loss of life or physical destruction. Examples often used are attacks on a nuclear power plant aimed at shutting down its cooling system and causing a Fukushima-type

46. Some authors refer to Chinese military doctrine in this respect. *See, e.g.*, Han Bouwmeester, Hans Folmer & Paul Ducheine, *Cyber Security and Policy Responses*, *in* CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 2, at 19, 36.

disaster, on an air traffic control system with the objective of causing a large number of aircraft to crash and on a flood control system triggering a massive and disastrous flood.[47] An attack such as one of those carried out by a nihilistic actor, e.g., Al Qaeda or one of its affiliates that had no regard for the consequences is potentially more plausible than an attack of this nature conducted by a State. Such an attack would undoubtedly rise to the level of an armed attack and it would not necessarily be part of the more comprehensive armed offensive that a State would be likely to employ.

A cyber "Armageddon" is not, however, as likely as sometimes suggested.[48] First, conducting a cyber armed attack on this scale is not readily within the capabilities of non-State organizations and obtaining the capability to do so is not easily accomplished. It would require a major effort, involving considerable time, technical and trained human resources, and probably the support of a State with sophisticated cyber capability for a terrorist organization to develop the capacity to achieve devastating results through the use of cyber alone. Second, the logical question is why a terrorist organization would make that effort when there are other more achievable means to produce similar results. Al Qaeda did not have to take over the air traffic control center at Kennedy International Airport in New York City to achieve the effect it did on 9-11. Instead it seized physical control of four aircraft, a capability more likely for a terrorist organization to possess than that necessary to initiate a major cyber attack. Nevertheless, although not likely, a major attack is feasible and the possibility of a terrorist organization obtaining the necessary capacity to conduct such an attack should not be discounted.

B. Responding to an Anticipated Cyber Armed Attack in Conformity with the Law

Having explored the likelihood of a cyber attack constituting an armed attack when conducted either in conjunction with the use of traditional kinetic military force or as a stand-alone attack, we next turn to an assessment of the manner in which the legal framework governing the exercise of the right of self-defense addressed in Section II would be applied in responding to a clear threat of a such an attack. We will do so on the basis of the conclusion reached previously that anticipatory self-defense is a lawful exercise of the right of self-defense when exercised in response to a manifest and

47. MYRIAM D. CAVELTY, CYBER-SECURITY AND THREAT POLITICS 2 (2007); RICHARD A. CLARKE & ROBERT KNAKE, CYBER WAR 64–68 (2010).

48. *See* Lawson, *supra* note 39.

unequivocal imminent threat of attack in the proximate future against a designated target State or States, as these criteria are laid down in the Charter and are contained in customary international law.

1. Combined Cyber and Kinetic Attacks

With regard to what we consider to be the most likely mode of cyber armed attack, namely, that occurring in conjunction with the use of kinetic force, there are no real differences from the manner in which the criteria for the exercise of anticipatory self-defense are applied to traditional means and methods of attack conducted without the use of cyber. The assessment of the likelihood of an imminent attack and the identification of the author of the attack, both based on credible evidence, and the gauging of a proportionate response would not differ in any meaningful way.

For example, if State A was clearly on the point of launching an attack against State B, and State B responded by launching a preemptive airstrike that destroyed a considerable portion of State A's air capability on the ground and command and control functions before the attack was launched, thereby gaining air superiority, it would make little or no difference whether either the attacking State A and/or defending State B employed or did not employ cyber weapons or techniques to assist their operations in terms of assessing the legality of the response.

The questions concerning the legality of the anticipatory response would be exactly the same with or without the use of cyber by either State. Was the evidence of an imminent attack credible? Were there available alternatives under the circumstances? Did the defender strike within the last feasible window of opportunity? Was the strike precipitate, therefore premature, because it was conducted before the evidence of attack was clear, before alternatives to the use of force were exhausted or before a determination was made that possible alternatives were not feasible under the circumstances? Was the response proportionate in relation to the reasonable evidence of the scope and nature of the threat?

The use of cyber weapons in such a scenario would have little or no influence on the answers to these questions and would, therefore, have equally little bearing on whether the response was in conformity with the law or not. In short, when cyber is employed alongside other means and methods of warfare, it will not significantly affect the outcome of an assessment of a preemptive response as a lawful or unlawful act of anticipatory self-defense.

The problem of identification of the potential attacker would not be increased if cyber weapons and techniques were employed in the attack since evidence of those preparations would be weighed together with physical indications of an impending attack. In fact, cyber activities might make identification of the attacking party easier if, for example, previous cyber espionage probes of the defending State's capabilities and deployments could be traced back to a State now demonstrating clear indications of preparation for an attack. This would be no different, in principle, from the use of electronic warfare techniques to intercept and decode messages indicating an attacking party's intentions.

2. Stand-alone Cyber Attack

In contrast to the cyber attack undertaken in conjunction with a kinetic attack, preparations for a stand-alone cyber attack would, in most cases, significantly affect the ability to act in anticipatory self-defense. To illustrate, assume actor A (a State or non-State actor) is on the point of launching the attack against State B and that State B is able to determine a digital attack on its critical infrastructure is being prepared. State B's right to launch a preemptive digital and/or kinetic defensive response in accordance with the criteria for the lawful exercise of anticipatory self-defense would depend entirely on its capacity to identify the prospective attacker and ascertain the attacking party's intentions and capabilities. In the absence of physical indicators, such as force deployments, aerial reconnaissance and intercepted communications, it would be exceedingly difficult, if not impossible, for a prospective target State to be able to identify the attacking party, ascertain the existence and nature of the threat, and gauge the necessary and proportionate response with a reasonable degree of certainty.

3. Accumulation of Events

There may be situations in which it is feasible for a State to determine the origin of an attack, perhaps because of reliable human or other intelligence, or other clear evidence, such as positive identification of the source of a prior attempt to carry out a similar, partially unsuccessful cyber attack. In that situation, the response would not be wholly anticipatory, since the attempted attack could be considered as continuing. This analysis would also apply to situations in which there had been a prior series of small-scale

digital attacks from the same source falling below the threshold of armed attacks that occur over a reasonably connected span of time—for example, a series of small-scale attacks to ascertain a defending State's vulnerabilities and capabilities. These attacks, taken together, comprise an attack of sufficient gravity to qualify as an armed attack justifying an exercise of self-defense to ward off the phased attacks and neutralize the threat of further attack.

Responding in self-defense to these small-scale digital attacks represents an application of the "accumulation of events" theory to a "*Nadelstichtaktik"* form of armed attack.[49] The defensive response in such a scenario would have both a reactive and anticipatory element, with the former predominating since it would be reacting to an ongoing attack, but it would also be forward looking by warding off further attack.

The importance of the anticipatory element would increase if the series of prior small-scale attacks clearly indicated a large-scale digital attack was imminent. In that case, a defensive response at the last window of opportunity before the attacker had completed preparations for launching the attack would qualify as an exercise of anticipatory self-defense. Whether it would qualify as a lawful exercise of anticipatory self-defense would depend on the credibility, reliability and sufficiency of the evidence and the absence of feasible alternatives, as well as the effort taken to ensure the response was proportionate to the threat.

4. Identification of the Author and the Threat

Probably the single greatest obstacle to the exercise of anticipatory self-defense in response to a stand-alone cyber armed attack is identification of the attacking party. A lawful exercise of anticipatory self-defense is an option only if reliable intelligence or other evidentiary factors enable the defending State to identify the prospective attacker and the nature and scope of the threat posed. The cyber domain is different from the physical one in a number of ways, but the one which is crucial in this respect is the relative degree of anonymity possessed by a prospective attacking party acting wholly within the cyber domain.

While the problem of identification of both the identity of the attacking party and the nature of the threat posed is real and substantial, it is not necessarily impossible to do so in at least some situations.

---

[49] *See supra* note 10 and accompanying text.

First, it may be possible to "hack-back" to obtain at least a preliminary indication where the attack originated. This will not necessarily be conclusive. Data travels over an entire network of connections and splits into data packages that traverse various geographic points and nodules. Even if the point of origin could be identified, the geographic source of a digital attack does not necessarily indicate the identity of the attacking party; it simply shows the data's originating location. If a digital attack utilized a so-called "botnet," of which there are many on the Internet, it would probably be unclear initially as to who or what was behind the attack, although this could become clearer after further investigation. However, any forcible response after the elapse of time required to establish the identity of the attacker would, in these circumstances, no longer be anticipatory. A more feasible alternative is prevention of the attack through the dismantling of botnets before they could be employed on the scale of an armed attack.[50]

That problem could be partially overcome by the fact that there are—at least at present and in the reasonably near future—relatively few States and even fewer, if any, non-State actors capable of mounting a wholly digital attack rising to the level of an armed attack, particularly one with potentially devastating consequences. This narrows the number of potential authors considerably, thereby making a positive identification of the source of the incipient attack more feasible.

Even with this narrowing, however, identifying the source of an incipient attack and determining the nature and scale of the threat pose significant, but not necessarily insurmountable, obstacles to the exercise of a lawful preemptive response when other more specific evidence of authorship is not present.

5. Preemptive Response

In sum, while anticipatory self-defense in response to an incipient armed attack that will employ both kinetic and cyber weapons and techniques is not substantially different from situations in which cyber operations are not part of the attack, there are significant obstacles to its exercise in reaction to a potential stand-alone cyber armed attack in the absence of clear intelligence or other factors enabling the defending State to identify the nature

50. For an example of the successful "take down" of a criminal botnet, see *Taking Down Botnets: Microsoft and the Rustock Botnet*, MICROSOFT ON THE ISSUES (Mar. 17, 2011, 6:36 PM), http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/03/18/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx.

and source of the attack. In some cases, there will be sufficient information to permit an anticipatory defensive response, but in others—perhaps the majority—there will not. This is a fact with which policy makers and military commanders must learn to live. There is, after all, no such thing as perfect security in the physical world either; surprise attacks have been carried out with varying degrees of success throughout military history.

This relative degree of uncertainty and the obstacles posed to the lawful exercise of anticipatory self-defense from a stand-alone cyber armed attack are real and cannot be wished away, but these factors do not preclude such action when they can be overcome and when other alternatives are neither feasible nor adequate to address the threat.

This uncertainty and these obstacles provide no reason to panic and certainly do not justify a weakening or changing of the law with regard to the exercise of anticipatory self-defense. Anticipatory self-defense is not frequently employed in the physical domain, with only a relatively few instances of it being exercised in response to more traditional modes of attack.[51] There is no reason why this should be different in the digital context.

Improvement of measures to enhance cyber security of vital military and civilian systems and the possession of adequate means of cyber defense, including the potential to carry out credible and effective cyber intelligence, will go far towards deterring a potential attack and limiting the effects of one, should it occur. Likewise, as stated earlier, the nature and scope of the threat of cyber attack should be kept in perspective; over reliance on preemption is not necessarily a way to increase cyber security. To the contrary, if used without proper attention to the well-established legal criteria governing the exercise of anticipatory self-defense, it could well increase the degree of "cyber insecurity" and needlessly escalate situations on the basis of misperceptions and miscalculations.

---

[51] While self-defense has an intrinsically anticipatory element that includes forestalling future attack, it is comparatively rare that the anticipatory element is exercised without an accompanying reactive element responding to a previously conducted attack. For example, the U.S. airstrikes on Libya in 1986 were designed to deter future attacks, but were also in response to the bombing of a Berlin disco in which U.S. service members were killed.

IV. SUMMARY AND CONCLUSIONS

We have detailed our reasons for concluding that the present legal framework governing the exercise of the right of self-defense is both relevant and applicable to cyber armed attacks. That framework provides a right of self-defense in response to either an ongoing or imminent armed attack within the conditions laid out in the UN Charter and under customary international law. The criteria of the Charter and customary law are complementary and apply to any invocation of the right of self-defense. This legal framework has long recognized the right to exercise anticipatory self-defense in response to a manifest and unequivocal threat of attack in the proximate future, within the general parameters of necessity, proportionality and immediacy. There is no reason to conclude the Charter eliminated this long-standing preexisting right. Anticipatory self-defense continues to be in force in the contemporary legal order as an intrinsic part of the larger notion of self-defense.

Anticipatory self-defense does not, however, permit so-called "preventive self-defense," i.e., the reaction to mere potential threats of attack that may or may not crystallize at some indeterminate point in the future, or action taken in the absence of credible evidence that an attack is imminent and establishing who or what is responsible.

Anticipatory self-defense includes the possibility of responding to an imminent armed attack that is wholly or partially conducted within the digital domain, provided the attack to be conducted would be on a comparable scale and have similar effects to a traditional kinetic attack carried out by a State. This would include situations where a cyber armed attack had the intended effect of resulting in more than nominal human casualties or causing significant physical damage and destruction through the direct secondary consequences of the digital attack. Additionally, in our opinion in those cases where the attack causes no direct physical effects, but where long-term, serious damage to digital systems controlling a State's critical infrastructure or essential functions resulted or was clearly intended, such action could constitute an armed attack justifying the exercise of self-defense when the damage was not capable of being remedied within a reasonable timeframe and the stability of a State and its society were seriously threatened.

In our view, anticipatory self-defense may be carried out in response to an imminent digital armed attack irrespective of whether the attack is conducted (1) by a State; (2) by a non-State actor acting either under the con-

trol, or with the substantial involvement, of a State; or (3) by a non-State actor acting alone.

We examined the probable modes by which an incipient cyber armed attack could be conducted and concluded that there are basically two modes. First, and increasingly the most likely, is in preparation for, or adjunct to, a traditional kinetic armed attack. In this case, the scope of a possible anticipatory defensive response would not be significantly affected, since it would be assessed in tandem with other physical indications of an impending attack. Second, a stand-alone cyber armed attack could occur justifying a proportionate anticipatory exercise of self-defense.

For a number of reasons, however, the stand-alone cyber attack is less likely to occur and less likely to warrant an anticipatory defensive response. First, most stand-alone cyber attacks fall well below the threshold of armed attack, which would preclude a use of force in self-defense. Second, even in cases where the level of the attack does reach the requisite legal threshold, in many—probably most—cases there will be insufficient knowledge of the author of the attack and its probable scope and intended effects to enable a reasonably accurate assessment of which State or non-State actor is responsible and to gauge the appropriate defensive response within the parameters of necessity and proportionality. Nevertheless, there could be limited situations in which sufficient information is available to enable a lawful preemptive defensive response to a stand-alone cyber attack. Although this option will not be available in many, indeed, probably most situations, that reality should not lead to panic and overreaction, or be used as justification for "bending the rules." Cyber attack is unlikely in most cases to require the exercise of self-defense. Even when it does, anticipatory self-defense is not necessarily the only or most appropriate response. Its use will be limited to those instances when it can be carried out with the least possible danger of miscalculation and when no other alternatives are feasible.

There are means other than the exercise of anticipatory self-defense in which cyber security can and should be improved and the effects of a potential attack deterred or limited. Overreaction or overreliance on preemption would be more likely to increase, rather than decrease, the level of "cyber insecurity." It would also undermine the legal framework for the use of force at great cost to all members of the international community.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

The Cyber Road Ahead: Merging Lanes and Legal Challenges

Kenneth Watkin

89 INT'L L. STUD. 472 (2013)

Volume 89 2013

The Cyber Road Ahead: Merging Lanes and Legal Challenges

Kenneth Watkin[*]

I. INTRODUCTION

It is a bit daunting to think about the "road ahead" when the concept of cyber warfare is just entering the public discourse. Fueled first by cyber "attacks" in Estonia and then in Georgia,[1] the dialogue has gotten louder with revelations about a cyber conflict occurring as part of the "covert" campaign to disrupt the nuclear program of Iran.[2] Terms such as "Stuxnet," "Duqu" and "Flame" have now entered the public cyber lexicon.[3] How international law should regulate the use of this technologically advanced domain with regard to the recourse to war (the *jus ad bellum*), and as method

* Brigadier-General, Canadian Forces (Ret.); Former Judge Advocate General for the Canadian Forces; 2011–12 Charles H. Stockton Professor of International Law at the U.S. Naval War College.

1. For an outline of cyber warfare in the twentieth and twenty-first centuries involving Israel, Chechnya, Estonia, Georgia, North Korea, Iran and the United States, see JEFFREY CARR, CYBER WARFARE 2–3 (2009).

2. Gary D. Brown, *Why Iran Didn't Admit Stuxnet Was an Attack*, 63 JOINT FORCE QUARTERLY 70 (2011), *available at* http://www.ndu.edu/press/why-iran-didnt-admit-stuxnet.html.

3. Nicole Perlroth, *Researchers Find Clues in Malware*, NEW YORK TIMES, May 31, 2012, at B1, *available at* http://www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stux net-and-duqu.html.

and means of warfare (the *jus in bello*) has become the subject of substantial legal scrutiny.[4]

The contemporary discussion of cyber threats speaks not only of danger, but often also of catastrophe. In this regard it is not uncommon to hear of cyber "Pearl Harbors"[5] and for cyber "weapons" to be equated to implements of mass destruction based on what has been termed a "microforce," similar to chemical and biological armaments.[6] In addition, it has been suggested that "[t]he conventions and applicable case law on nuclear warfare are relevant to controlling the scope and tools of [information warfare]."[7] The use of the term "information warfare" reflects an almost schizophrenic discussion that includes soft concepts like preserving or exploiting information, and bellicose words, such as attacks.[8]

As a microforce, cyber presents a significant communication challenge for anyone attempting to explain how it works and why anyone should be worried about its capabilities. It is difficult to suggest that cyber is a threat of exceptional proportions when cyber means are trending in the opposite direction with ever shrinking hardware. Explanations of the cyber domain often result in a dialogue wrapped in a mysterious language of "clouds," "viruses" and "botnets." Reflecting its nascent status in terms of regulation, the language of cyber incorporates a breathtaking range of seemingly un-

---

4. *See* TALLINN MANUAL ON THE LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013); CYBER WARFARE: CRITICAL PERSPECTIVES (Paul Ducheine et. al. eds., 2012).

5. Jason Ryan, *CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor*, ABC NEWS (Feb. 11, 2011), http://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905#.UHLoS7SqCME.

6. In assessing "digital warfare," one the author notes:

> Compared to other types of military force, digital warfare represents a type of microforce. The distinction is analogous to the difference drawn between conventional military forces employing chemical explosives or kinetic energy as their primary means of achieving effect versus the megaforce unleashed by nuclear weapons based on the fission or fusion of atoms. At issue here is the amount of energy unleashed by a given weapon at the time of attack. Weapons across the micro-conventional-mega force spectrum can all cause very significant impacts. Chemical or biological weapons are referred to as weapons of mass destruction, not because of the amount of destructive energy released when they are deployed but because of the number of deaths they can cause. . . . Despite the microforce nature of information attacks, disruption of the digital control systems of a nuclear power plant could cause similarly large-scale effects.

GREGORY RATTRAY, STRATEGIC WARFARE IN CYBERSPACE 20 (2001)

7. *See also* Scott J. Shackleford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKLEY JOURNAL OF INTERNATIONAL LAW 191, 217 (2009).

8. *Id.* at 198–99.

connected concepts that appear more closely aligned to advertising, science fiction and biological threats, although it can also take on a more bellicose connotation in its reference to attacks. This language can be problematic for those seeking to come to grips with the domain and, importantly, communicate its dangers within governments and to the broader public.

At times, there can be an overriding sense that the public is only now learning what States are being forced to reveal.[9] Cyber is a creature of technological advancement. As often occurs, the technology has developed well ahead of the limiting framework States use to keep its advances in check. In this regard, the road ahead appears to be one with two merging lanes. One path is a technological, with advances occurring at apparently prodigious speed. Such developments are limited, it would seem, only by the imagination of their creators. The other lane is one where the policy, ethical and ultimately legal constraints of society are being test driven even as they are being developed. In a sense this is a phenomenon that has been seen before as society struggled to control the development of chemical and nuclear weapons and air warfare following World Wars I and II.

However, there is a fundamental difference in the twenty-first century. At no point were the twentieth century weapons readily available to the world's population. It was estimated in 2008 there were one billion personal computer users worldwide, a figure expected to double by 2014.[10] Among those users are teenagers keen on social networking or testing their ability to challenge the rules imposed on them by society. It is a world that also includes hacktivists, like the group Anonymous, whose penetration of government, business and organizational websites raises security concerns, but is not readily associated with legal concepts such as armed attack and armed conflict.[11]

---

9. Scott Shane, *Cyberwarfare Emerges From Shadows for Public Discussion by U.S. Officials*, NEW YORK TIMES, Sept. 27, 2012, at A10, *available at* http://www.nytimes.com/2012/09/27/us/us-officials-opening-up-on-cyberwarfare.html?pagewanted=all ("Just as drone-fired missiles have never been a secret to those on the ground, so cyberattacks have consequences that cannot be hidden, even if their origin may be initially uncertain.").

10. *Computers in use pass 1 billion mark: Gartner*, REUTERS (June 23, 2008), http://www.reuters.com/article/2008/06/23/us-computers-statistics-idUSL2324525420 080623.

11. Devlin Barret, *Retaliation Fears Spur Anonymity in Internet Case*, WALL STREET JOURNAL, Jan. 28, 2012, at A3, *available at* http://online.wsj.com/article/SB10001424052970203363504577185364 230417098.html ("Anonymous is a loose affiliation of hackers and activists who are self-proclaimed protectors of Internet freedom. To the Justice Department, the group is something more sinister. More than a dozen alleged members have

The "information superhighway" that forms the backbone of the cyber domain is truly a crowded thoroughfare.[12] What is not known at this stage is whether the intersection of the two lanes along this cyber road stretching into the future will be the scene of a tremendous clash of cultures (one technological and the other societal) or a seamless integration that restricts cyber as a means of warfare to help meet the security needs of States, while being constrained by humanitarian demands in its application.

One can be skeptical regarding the accuracy of the forecasts of cyber Armageddon with the advent of cyber warfare. Although it has largely now disappeared from the contemporary cyber dialogue, in 1999 there were predictions by the technical community of a potential "catastrophe." However, this one was in the nature of a self-inflicted wound. Apparently, in the early days of computer development:

> [P]rogrammers sought to economise on then-scarce computer storage space by writing dates with two digits for the year instead of four. These programmers either failed to consider the implications of the end of the 20th century or assumed that their systems would have been scrapped long before then. By the time the problem was taken seriously in the mid-1990s, code with two-digit dates was said to be ubiquitous, occurring not only in conventional computer systems but in 'embedded systems' such as those in automatic lifts, air navigation systems and so on. While the exact consequences of these problems were beyond anyone's imagination, widespread system failures could be anticipated on 1 January 2000, and the cascading effect of these failures was expected to cause, at a minimum, severe economic dislocation.[13]

The Y2K concern is of particular relevance to twenty-first century discussions about cyber warfare. It involved the resilience of the machines and systems, such as the supervisory control and data acquisition (SCADA)

---

been charged with computer crimes; they have pleaded not guilty. Anonymous has no formal structure or membership, and in some ways is more of a banner under which hackers and others choose to operate than an actual organization.").

12. "Information superhighway" is defined as "an extensive electronic network such as the Internet, used for the rapid transfer of information such as sound, video, and graphics in digital form." OXFORD DICTIONARIES ONLINE, http://www.oxforddictionaries.com (last visited Oct. 3, 2012).

13. John Quiggan, *Y2K Scare: Causes, Costs and Cures*, 64 AUSTRALIAN JOURNAL OF PUBLIC ADMINISTRATION 46 (2005), *available at* http://www.uq.edu.au/economics/johnquiggin/JournalArticles05/QuigginAJPA05Y2K.pdf.

networks controlling electrical grids and pipelines,[14] and the impact of a critical failure of these machines that govern everyday life and harness the dangerous forces upon which modern civilized society is based.[15]

The result was a mobilization of large parts of the developed world to prepare for the turn of the century. In November 1999, it was estimated expenditures "by U.S. firms, non-profits and government agencies, in the years 1995 through 2001, will be in the neighborhood of $100 billion, or about $365 per U.S. resident."[16] Apparently the response was not uniform, as Europe and other parts of the world either reacted unenthusiastically or not at all.[17] In contrast, English-speaking countries paid particular attention to the perceived threat, not only because of their common language and historical ties, but also, it is suggested, as a result of reliance to various degrees on tort litigation as a means of social regulation.[18]

The rest is history, as uneventful as it was. The predictions proved very wrong. Perhaps the best summary is that provided by John Quiggan, who noted with regard to the Y2K "disaster" that "[f]rom the perspective of public administration, the two most compelling observations relate to conformity and collective amnesia."[19] Once a conformist response has been initiated, "no policy actors have any incentive to oppose, or even to critically assess, the dominant view."[20] Developed countries had become dependent upon new technology that apparently was not fully understood. This

---

14. For an outline of the threat that computer malware and hackers could have on SCADA systems, see RICHARD A. CLARKE & ROBERT K. KNAKE, CYBERWAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 98–101 (2010).

15. ECONOMICS AND STATISTICS ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE, THE ECONOMICS OF Y2K AND THE IMPACT ON THE UNITED STATES 7 (1999), *available at* http://www.esa.doc.gov/sites/default/files/reports/documents/y2k_1.pdf [hereinafter *United States Y2K Report*] (describing that "critical infrastructure . . . suggests facilities whose damage due to Y2K failures would cause a wide circle of disruptions. Damages may still essentially be local, however. In an economy as large as the United States, hundreds and perhaps thousands of failures in 'critical infrastructure' electricity or water systems could occur before the impact would be great enough before there would be a significant impact.").

16. *Id.* at 11.

17. Quiggan, *supra* note 13, at 49 ("The response to Y2K problems in non-English speaking countries was slower and less enthusiastic. . . . In Eastern Europe and less developed countries, the Y2K problem was almost entirely ignored in view of the more pressing concerns facing these countries.").

18. *Id.* at 53.

19. *Id.* at 54.

20. *Id.*

led to a perceived crisis. The Y2K incident suggests, perhaps, that with regard to claims regarding the impact of cyber warfare it would be prudent for legal advisors to have a degree of skepticism in assessing predictions of disaster.

Much has changed, however, since Y2K. Cyber is even more integrated into society. As a security issue, it is here to stay and appears to be capable of more than simple interference with our lives. Indeed, in addition to being integrated into our everyday life, cyber is also part of the national order of battle for over thirty countries.[21] It is assessed that at least twelve of the world's fifteen largest militaries are building cyber warfare programs."[22] For the United States, this means cyberspace is an operating domain on par with land, sea, air and space,[23] as well as one requiring dedicated command and units.[24] It is likely that the involvement of other countries in the military cyber realm will be considerably more modest. What is unclear is the degree to which cyber "have" countries will be, rightly or wrongly, more concerned with cyber threats and the dangers they pose because of risks to military capabilities or broader economic interests.[25]

Like Y2K, there is a danger that overemphasis on predictions of catastrophe will heavily influence how the threat is perceived and responded to by a State. The perception of the threat may also be affected by the tools available to the State to respond. This could mean that in countries without the same level of dedicated military resources as some developed countries the cyber challenge could be viewed as less military in nature. It may more naturally lead to discussion of alternatives to the use of force and increased international dialogue and cooperation. Of course, the challenge facing policy makers is whether those options are sufficient to confront the threat.

At the same time other States, which have not—or cannot—develop sophisticated cyber capabilities, may also have a particular interest in ensuring international law operates as a brake on the cyber warfare activities of the "have" States. There is nothing new in using the law for that purpose. It has been at the heart of the post-World War I and -World War II em-

---

21. INTERNATIONAL INSTITUTE FOR SECURITY STUDIES, THE MILITARY BALANCE 2011, at 27, 28–32 (2011) (assessing the military dimension of cyberspace).

22. Shane, *supra* note 9.

23. U.S. DEPARTMENT OF DEFENSE, QUADRENNIAL DEFENSE REVIEW REPORT 37 (2010).

24. *Id.* at 38–39.

25. *Id.* at 37 ("In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace.").

phasis on the *jus ad bellum* restrains on the recourse to war.[26] Therefore, while countries like the United States may seize the opportunity to shape the international legal discussion regarding regulation of the cyber domain, so will those countries that seek to reinforce the need for restraint.[27] In this respect, international law will need to reflect standards that apply to all countries.

In any event, all military cyber forces and their legal advisors will be faced with a number of challenges as the march down the cyber highway proceeds. The challenges can be placed into two broad categories: first, the prevalent, indeed predominate non-military use of cyber in society. Second, in a dialogue that is just starting to take place in a public way, is the need to reach consensus on how the international law can and should bring a potential technical "beast," made of "1s" and "0s," to heel on this very human journey down the cyber roadway. If the predictions of catastrophe are true, this makes the need for regulation all the more pressing. However, as will become evident, efforts to provide law and order in the cyber world will be challenged by the fact that as a policy option the use of cyber to influence the security environment seems so attractive.

This article will address these challenges in three parts. First, there will be an outline of a unique aspect of the cyber domain in the context of its status as a new global commons and its prevalence within modern society. As a result there will be many stakeholders who have views that will impact on the regulation of cyber activity. Second, the analysis will turn to specific legal challenges. This part will look at civilian participation in cyber conflict, consider the theoretical approaches applied when assessing cyber operations as a use of force, look at the use of the cyber domain for countermeasures short of war and address the significant potential for confusion at a foundational level regarding the use of the term "attack." Finally, the potential for successfully integrating cyber operations into a legal framework will be considered by reference to efforts during the twenty-first century to regulate technologically advanced aerial warfare. Ultimately the road ahead

26. Quincy Wright, *The Outlawry of War and the Law of War*, 47 AMERICAN JOURNAL OF INTERNATIONAL LAW 365, 368 (1953).

27. Shane, *supra* note 9 (Where Matthew Waxman is said to have noted that, whereas previous United States administrations had ceded ground to critics by remaining silent on drones and therefore allowing them to be portrayed as lawless, the U.S. government is now being more public with regard to cyber issues. As the United States "occupies a position of advantage on offensive cyber capabilities, it should seize the opportunity to lay out a set of rules for itself and others.").

will be identified as a challenging one, but with an attainable goal that will require flexibility in applying traditional legal principles to the cyber domain.

II. A VOICE AT THE TABLE?

A key challenge for those seeking to attract the attention of lawyers and policy makers regarding the dangers and opportunities of military cyber capabilities is getting a voice at the table that is heard and understood. To get a sense of the scope and scale of the challenge, it is useful to look at national policies regarding cyber. Consistent with the United States having an advanced cyber capability and the openness inherent in it being a democracy, that country has a number of publically available defense related documents on the issue.[28] It is the overarching 2011 national strategy document *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* that broadly defines the nature of the international cyber challenge.[29] It states:

> [D]igital infrastructure is increasingly the backbone of prosperous economies, vigorous research communities, strong militaries, transparent governments, and free societies. As never before, information technology is fostering transnational dialogue and facilitating the global flow of goods and services. These social and trade links have become indispensable to our daily lives. . . . The reach of networked technology is pervasive and global. For all nations, the underlying digital infrastructure is or will soon become a national asset.[30]

Of course, States must defend their national assets; however, this statement raises a number of profound issues. Can a State physically defend all of its national digital assets? What is the cost in terms of global discourse and, in particular, international commerce? If national assets are defended will it mean reduced, or even truncated, access to the computer sys-

---

28. *See, e.g.,* QUADRENNIAL DEFENSE REVIEW REPORT, *supra* note 23; U.S. DEPARTMENT OF DEFENSE, DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf.

29. THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter *International Strategy for Cyberspace*].

30. *Id.* at 3.

tems that underpin the information superhighway for global participants? There is also the more mundane bureaucratic question of who needs to be sitting around the table at the highest levels of government to make those decisions in order to ensure the military imperatives are properly weighed against the economic and social costs of seeking to regulate the cyber domain.

Another fundamental issue is whether national assets effectively lose their parochial status because they are part of an interconnected network that "is pervasive and global."[31] Is the legal control of the digital world "territorial" in the sense of coming exclusively under State sovereignty? To a certain extent the answer to this question is yes. The international legal framework is founded on the concept of the post-Westphalian State. It simply makes sense that the regulation of a fundamentally international technology would be State-based and State-focused as well. This is not to take away from the role that international institutions play or the impact of increasing globalization, however, States "retain their attraction as the primary focus for the social activity of humankind and thus for international law."[32]

But the boundaries of national jurisdiction in the cyber world are not clear. The cyber environment can be equated to a global commons, such as the oceans, although it has also been noted that "unlike the other domains, cyberspace has no physical obstacles, nor 'real' boundaries like a shore."[33] The cyber domain is also unique in that it is manmade.[34] International regulation of the maritime domain has been slow but steady, as it has had to balance the rights of States, territorial jurisdiction, freedom of navigation and private economic interests. It has been noted that "[t]he story of the evolution of [the UN Convention on the Law of the Sea] is the imperative that the private sector must be given a place if real progress in regulating the commons is to be made."[35] Ultimately, the regulation of global commons, as is evidenced by the law of the sea, "ha[s] a significant effect on the exercise of both belligerent and neutral rights during time of armed

31. *See International Strategy for Cyberspace, supra* note 29, at 3.

32. MALCOLM N. SHAW, INTERNATIONAL LAW 197 (6th ed. 2008).

33. Frans Osinga*, Introducing Cyber Warfare,* in CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 5, at 9.

34. QUADRENNIAL DEFENSE REVIEW, supra note 23, at 37.

35. Shackelford, *supra* note 7, at 226.

conflict."[36] Private, particularly commercial, interests in the cyber domain will also have to be taken into account in the regulation of cyber conflict in much that same way that neutrality has impacted on international humanitarian law.[37]

Further, not all States have embraced international regulation of the oceans. While a State, like the United States, may have a significant interest in adopting the United Nations Convention on the Law of the Sea (UNCLOS), conflicting ideas of national security interests have prevented it from doing so.[38] The United States military supports ratification.[39] Rather than be bound by such regulation, however, a certain advantage has been perceived within the legislative branch of the United States government in the constructive ambiguity of having an international regime in place, but not being technically subject to its constraints.[40] The same result could occur regarding a number of the players in the cyber domain. Ambiguity often equates to freedom of action. Freedom, however, can come at the expense of other States understanding the motives and the potential action to be taken by a nation. It can also impact adversely on the issue of accountability.

It is also not clear how—or if—States and their military forces will want to embrace international regulation when the use of cyber for military

---

36. SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA 93 (Louise Doswald-Beck ed., 1995)

37. LESLIE GREEN, THE CONTEMPORARY LAW OF ARMED CONFLICT 297 (3d ed. 2008) ("Even in major conflicts involving a number of countries, including the most powerful, there are always some which remain outside the conflict and seek to assert their right as neutrals not to be interfered with by the belligerents.").

38. Thomas Wright, *Outlaw of the Sea*, FOREIGN AFFAIRS (Aug. 7, 2012), *available at* http://www.foreignaffairs.com/articles/137815/thomas-wright/outlaw-of-the-sea (Describing that the two objections in the United States Senate regarding ratification of UNCLOS are concerns over encroachment of the International Seabed Authority on United States sovereignty and "the treaty would prevent the U.S. Navy from undertaking unilateral action, such as collecting intelligence in the Asia-Pacific region, because permission to do so is not explicitly granted in the text").

39. *Id.* ("According to Admiral Samuel Locklear, commander of U.S. Pacific Command, however, the convention in no way restricts our ability or legal right to conduct military activities in the maritime domain. On the contrary, as U.S. Defense Secretary Leon Panetta puts it, U.S. accession to the convention 'secures our freedom of navigation and overflight rights as bedrock treaty law.'").

40. *Id.* ("[C]ritics point out, the ultimate indispensability of U.S. naval power means that the country can receive the benefits of the convention without being bound by it. Since the world seems to have functioned perfectly well in this halfway house for some time, it would make no sense to codify the convention now.").

operations has yet to be fully developed or exercised. Such reluctance may also impact the decisions of less dominant States that want to avoid controls on its use favored by a more dominant cyber power. A military cyber capability provides a potential asymmetric advantage that may be simply too attractive an option for those States seeking to level the security playing field.[41] As John Arquilla has noted, "[n]o country may be foolish enough to engage the incomparable U.S. military in open battle, but we seem like fairly easy pickings to the computer mice that may soon roar."[42] Rather, the pressure for regulation may ultimately come from major industrialized States once they feel threatened, since "dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by non-state actors."[43]

Given the pervasive role played by the cyber domain in modern society, it also is unlikely that national security law and policy makers will unilaterally determine the outcome of the cyber debate. The interests of individual States and the views of their military forces on what is needed for defense will be just two of the many voices at the table to discuss what, if any, rules are established to regulate the defense of the national cyber systems.[44] One issue will be the relative importance States place on potential threats in a defense context in relation to very real non-military cyber threats that States presently face. For countries, such as the United Kingdom and Canada, the relatively low prioritization of the cyber challenge in terms of defense is reflected in the limited space their national cyber strategies devote to the topic. Further, in reading national policies' references to "defense," the term cannot be assumed to have a military context as it often means protection against criminal activity and espionage. Substantive reference to

41. Richard Stiennon, *Is An International Cyber Regulatory Agency Needed?*, FORBES (Aug. 22, 2012), *available at* http://www.forbes.com/sites/richard stiennon/2012/08/22/is-an-international-cyber-regulatory-agency-needed/ ("I can imagine that the concept of such a treaty and regulatory body will not gain much traction in the military academies and think tanks around the world. Why restrict a nation's options in war fighting—especially when cyber weapons are inexpensive (compared to fighter jets, tanks, and aircraft carriers) and could reduce the overall level of force required to achieve an end goal?").

42. John Arquilla, *Cool War*, FP NATIONAL SECURITY (June 15, 2012), http://www.foreignpolicy.com/articles/2012/06/15/cool_war.

43. Osinga, *supra* note 33, at 10.

44. For an outline of the divergent views and priorities of bureaucratic actors when considering policy priorities "amid a rapidly evolving strategic environment," see Mathew Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4),* 36 YALE JOURNAL OF INTERNATIONAL LAW 421, 436 (2011).

cyber and the role of military forces is usually found somewhere towards the back of the strategy.[45]

Although there appears to be much to defend in terms of its priorities, the subject of defense competes for space with privacy, business security products, cyber crime, cyber fraud and even the denial of safe havens to cyber criminals.[46] It appears that consideration of cyber "national defense," using the term in a *jus ad bellum* context, and the law that frames it in the post-UN Charter world, have been introduced rather late into the journey down the cyber roadway. This raises questions as to whether States have actually viewed the military threat to be as a grave as some would suggest, or whether it is criminal activity that is seen to form the most significant challenge.

The focus on issues other than cyber warfare is a reality and, in many respects, so it should be. Most citizens are more concerned with losing money from their bank account or a lowering of their credit rating than being the subject of an actual armed cyber attack that would cause the Security Council to meet to discuss two States having gone to war.[47] Cyber is different. More citizens rely on, and can relate to, the cyber realm. It is the predominance of cyber in the everyday lives of developed and, increasingly, less-developed States that will put considerable pressure on lawyers to closely consider how traditional security related concepts and principles of international law apply to this new form of warfare.

III. THE LEGAL CHALLENGE

A. Participation in Cyber Conflict

When thinking about the cyber domain, lawyers who work with national defense issues, in particular the use of military force may be challenged to rethink long-held notions of international law. For example, one area that

45. *See, e.g.,* CABINET OFFICE, THE UK CYBER SECURITY STRATEGY PROTECTING AND PROMOTING THE UK IN A DIGITAL WORLD ¶ 4.9 (2011), *available at* http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf [hereinafter *UK Cyber Security Strategy*]; GOVERNMENT OF CANADA, CANADA'S CYBER SECURITY STRATEGY: FOR A STRONGER AND MORE PROSPEROUS CANADA 3 (2010), *available at* http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf [hereinafter *Canada's Cyber Security Strategy*].

46. *See UK Cyber Security Strategy*, *supra* note 45, at 26; *Canada's Cyber Security Strategy*, *supra* note 45, at 12–13.

47. U.N. Charter art. 51.

may be impacted by the unique aspects of cyber warfare is the concept of legitimate participants in warfare. A hallmark of contemporary international law and war is the separation of the rules governing the conduct of warfare from those constraining the recourse to war.[48] While it is important to have the *jus ad bellum* considered separately from the *jus in bello* (or international humanitarian law) in order to maintain the "equal application" principle regarding the rules that govern warfare, that cannot always be easily done. This is particularly evident regarding the status of persons taking part in hostilities. The breadth of civilian involvement in the cyber domain, both inside and outside of government, will place even greater stress on traditional notions of legitimate participation in armed conflict.

One of the challenges arising from the twentieth century obsession with restricting inter-State armed conflict has been that the *jus ad bellum* has come to be associated narrowly with national self-defense. However, reflecting its roots in just war theory, the *jus ad bellum* contains a number of other fundamental principles, such as fighting for the "proper authority."[49] The application of this principle leads, at times, to a continuing interaction between *jus ad bellum* and *jus in bello* that is perhaps most obviously displayed when legitimate participation in conflict is assessed. If you fight for the "proper authority" (i.e., a State) then you are "legitimate," having both the right to participate in armed conflict and gain the protected status of prisoner of war. This legitimate status is recognized in foundational humanitarian law treaty documents.[50] In addition, while the *jus ad bellum* is traditionally viewed not as being applicable to non-international armed conflict,[51] the principle of proper authority effectively makes those mem-

48. YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 3 (2d ed. 2010) ("The fundamental postulate of the *jus in bello* is the equal application of its legal norms to all Belligerent Parties, regardless of their relative standing in the eyes of the *jus ad bellum*.").

49. JAMES TURNER JOHNSON, MORALITY AND CONTEMPORARY WARFARE 30 (1999) (outlining the *jus ad bellum* principles found under positive international law as being: just cause, right or proper authority, right intention, proportionality of ends, last resort, reasonable hope of success and the aim of peace).

50. *See* Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. IV Respecting the Laws and Customs of War on Land arts. 1–3, Oct. 18, 1907, 36 Stat. 2227; Convention (III) Relative to the Treatment of Prisoners of War art. 4.A, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135.

51. Marco Sassoli, Ius ad Bellum *and* Jus in Bello—*The Separation between the Legality of the Use of Force and Humanitarian Rules to be Respected in Warfare: Crucial or Outdated?*, *in* INTERNATIONAL LAW AND ARMED CONFLICT: EXPLORING THE FAULTLINES 241, 254 (Michael N. Schmitt and Jelena Pejic eds., 2007) ("Technically, no international *jus ad bellum*

bers of the security forces who fight for States the legitimate actors in such conflicts. It is the non-State actors whose activities are criminalized.[52]

That said, one of the realities of the cyber domain is that combatants in international armed conflict and security personnel in internal ones cannot defend all the national digital assets on their own. Those assets, and the threats posed to them, are too numerous and broadly distributed.[53] In many respects cyber activity represents a true expansion of the "home front" as an area of operations, even into the boardrooms and bedrooms of the nation. To the extent the introduction of airpower represented a kinetic means by which State-directed violence could be extended to a broad range of targets beyond national borders, cyber provides an even more expanded and in some ways more intimate threat.

As a result, many of the potential participants in this cyber war are likely not to be wearing uniforms or bearing arms, at least in the traditional sense. Due to its scope and scale, this represents a civilian involvement that appears significantly more challenging in terms of assessing its legitimacy than the contemporary controversy regarding Central Intelligence Agency personnel conducting drone strikes.[54] This leads to fundamental questions regarding the status of civilians who man the computer defenses of a State. Are they direct participants in hostilities? Do they really have to wear a uniform and be sworn into the armed forces of the State to lawfully participate in these activities? The answers may simply be that they are legitimately carrying out the responsibilities assigned to them in the same fashion as the police officers that arrested German saboteurs who had surreptitiously

---

exists concerning non-international armed conflicts, since such conflicts are neither justified nor prohibited by international law.").

52. *See* G.I.A.D. DRAPER, THE RED CROSS CONVENTIONS 14 (1958) (discussing attempts at the end of World War II to extend the provisions of the Geneva Conventions to internal conflicts and noting that "proposals giving insurgents a legal status, and consequently support, would hamper the Government in its measures of *legitimate* repression") (emphasis added).

53. Paul Ducheine, Joop Voetelink, Jan Stinissen & Terry Gill, *Towards a Legal Framework for Military Cyber Operations*, *in* CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 5, at 106 ("Given the characteristics of the threats as well as the 'battlefield' . . . , governments alone are incapable of responding adequately as they are heavily dependent upon private partners such as internet providers.").

54. Andrew Burt & Alex Wagner, *Blurred Lines: An Argument for a More Robust Legal Framework Governing the CIA Drone Program*, 38 YALE JOURNAL OF INTERNATIONAL LAW ONLINE 1 (2012), http://www.yjil.org/docs/pub/o-38-burt-wagner-blurred-lines.pdf.

landed on the shores of the United States during World War II[55] or Jose Padilla when he landed in Chicago in 2002.[56] In complying with the requirements of domestic law in the performance of their duties, they are not illegitimate under international law. Nor should they be liable to foreign prosecution for doing so. Indeed, it would have been an odd result to suggest that any apprehension of the saboteurs, who in today's terminology were unprivileged belligerents, had to be carried out by United States military personnel regardless of the geographic location.

The widespread involvement of civilians in the defense of computer networks could once again put the fundamental humanitarian law principle of distinction under pressure. In this instance, it will not be the factory workers of World War II who are considered to be "quasi-combatants," but rather potentially those who maintain the integrity and security of computer networks in their everyday employment.[57] It will be difficult to say that those civilians are far away from the battlefield when the cyber conflict is occurring literally in their laps. In this respect, they are different than the third echelon civilian supply workers or strategic level intelligence analysts who often seem to get a "geographic" pass when direct participation in hostilities (DPH) is considered. Cyber participants may be harder to separate from the action that is occurring literally at their fingertips.

The International Committee of the Red Cross, in its *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, appears to avoid this issue by concentrating on computer network attacks against military systems[58] and the offensive use of cyber.[59] That *Interpretive Guidance* notes that for "remote-controlled (i.e. geograph-

55. LOUIS FISHER, NAZI SABOTEURS ON TRIAL 33–36 (2d ed. 2005) (outlining the arrest of the saboteurs).

56. *See* Donna Leinwand & Jack Kelley, *U.S. Citizen Arrested in 'Dirty Bomb' Plot*, USA TODAY (Nov. 6, 2002), *available at* http://usatoday30.usatoday.com/news/nation/2002/06/10/terror-arrest.htm

57. In seeking to justify attacks on factory workers as quasi-combatants, a practice no longer permitted under international law, one author explained:

> It is not a question of political or moral support, or even of material support in forms that could not possibly be called warlike. What justifies the deliberate attack on the people concerned is that they are engaged in work which his akin to that done by uniformed men in the field. They are helping to pass the ammunition.

J.M. SPAIGHT, AIR POWER AND WAR RIGHTS 47 (3d ed. 1947).

58. INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 48, 50 (2009) [hereinafter *Interpretive Guidance*].

59. *Id.* at 55, 68.

ically remote) missiles, unmanned aircraft and computer network attacks," the "causal relationship between the employment of such means and the ensuing harm remains direct regardless of temporal or geographical proximity."[60] The legal and practical challenge is that the symbiotic relationship between offense and defense means the two concepts cannot be readily divorced. As a result, participation in the defense of computer systems raises the specter of DPH.

The transformative nature of cyber is reflected in the example of a fifty-nine-year-old retired grandmother who was reported in a Canadian newspaper in June of 2011 to be passing on information obtained through the social media site Facebook to a NATO twitter account. The information was said to include the coordinates of Colonel Gadhafi's forces' temporary headquarters in Libya, "along with the longitude and latitude for other targets."[61] The woman lived in central Canada just north of the United States border, obviously a considerable distance from the Libyan battlefield.[62] Another person passing on details regarding fuel tankers at a Libyan port was reported to be a forty-eight-year-old ice cream business supervisor in Arizona.[63] Is a person who takes information posted by someone else from the web and passes it on taking a direct part in hostilities? The *Interpretive Guidance* makes a link between the transmittal of tactical intelligence and the potential causation of harm resulting from any targeting decision.[64] Scenarios such as these raise questions of degrees of remoteness and where the line will be drawn on cyber DPH.[65]

In any event, so what if civilians are involved in cyber conflict? Such participation is not illegal under international humanitarian law unless it engages issues of perfidy, although some activity does theoretically raise

---

60. *Id.* at 55.

61. Graeme Smith, *How social media users are helping NATO fight Gadhafi in Libya*, GLOBE AND MAIL (Canada) (June 14, 2011), *available at* http://www.theglobeandmail.com/news/world/how-social-media-users-are-helping-nato-fight-gadhafi-in-libya/article583325/.

62. *Id.*

63. *Id.*

64. *Interpretive Guidance*, *supra* note 58, at 54–55 ("More precisely, where a specific act does not on its own directly cause the required threshold of harm, the requirement of direct causation would still be fulfilled where the act constitutes an integral part of a concrete and coordinated tactical operation that directly causes such harm.").

65. Smith, *supra* note 61 (noting "[a] Twitter account with apparent links to the British military has even taken the unusual step of asking users to submit the precise co-ordinates of troops loyal to Colonel Moammar Gadhafi").

questions of prosecution under the domestic jurisdiction of an opposing State if a participant is ever captured.[66] It also does not mean there could not be other potential consequences. For example, the operators of unmanned drones are located in the United States and the strikes are occurring in Afghanistan, Iraq and elsewhere on the other side of the globe.[67] Cyber connectivity means, however, that direct participants may be subjected to a cyber response, although likely one leading to a denial-of-access or disabling of means rather than one that is destructive in nature.

If it is not participants themselves, then the State in which they are operating may draw the attention of the targeted State. This is not necessarily problematic when that State itself is already a belligerent in the armed conflict. However, for the States that conducted the bombing campaign in Libya, it might have come as a shock if a cyber response from the government of Libya had been directed at them from so far away. In other situations where the State has no intentions of being a belligerent, the global nature of cyber has the potential to engage the responsibility of States for activities emanating from their territory much more broadly and swiftly than in the past. For example, it is reported that when it was subjected to distributed-denial-of-service (DDoS) attacks against its websites during the 2008 conflict with Russia, Georgia transferred official Internet assets to the United States, Estonia and Poland.[68] This has raised questions regarding United States neutrality. In this respect, "[t]he fact that American IT companies provided assistance to Georgia, a cyber belligerent, apparently without the knowledge or approval of the U.S. government, illustrates what is likely to become a significant policy issue."[69]

---

66. *See* ALLAN ROSAS, THE LEGAL STATUS OF PRISONERS OF WAR: A STUDY IN INTERNATIONAL HUMANITARIAN LAW APPLICABLE IN ARMED CONFLICT 305 (1976) (explaining that a person not having the status of lawful combatant "may be punished under the internal criminal legislation of the adversary for having committed hostile acts in violation of its provision (e.g. for murder), even if these acts do not constitute war crimes under international law"). *See also* DINSTEIN, *supra* note 48, at 35–39 (discussing the consequences of unlawful combatancy).

67. *See* Elizabeth Bumiller, *A Day Job Waiting for a Kill Shot a World Away*, NEW YORK TIMES, July 30, 2012, at A1, *available at* http://www.nytimes.com/2012/07/30/us/drone-pilots-waiting-for-a-kill-shot-7000-miles-away.html?pagewanted=all; MATT J. MARTIN, PREDATOR REMOTE-CONTROL AIR WAR OVER IRAQ AND AFGHANISTAN: A PILOT'S STORY 30 (2010).

68. Stephen W. Korns & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, PARAMETERS, Winter 2008, at 60, 60.

69. *Id.* at 61.

If civilian participation in cyber warfare from either an offensive or defensive perspective is seen as problematic, what is the true role for those in uniform and those who wear more casual attire? Given the nature of the medium, the scope of the activity and the importance of the information, it appears that international lawyers are not going to easily put such "unprivileged" participation back in the traditional combatant box. And given this interface with citizens on the domestic front, the discussion inevitably will not be just about the separation of *jus ad bellum* and *jus in bello*, or who can fight or not, but also domestic privacy, criminal law, and human and civil rights. This ultimately will require a more holistic application of the law impacting on operations. Perhaps this requirement to consider the broader implications of cyber conflict will force an application of operational law spanning numerous legal disciplines rather than deal with the issues compartmentalized into traditional legal silos.[70]

International lawyers are also going to have to be prepared to explain to a varied group of colleagues, both lawyers and non-lawyers, why combatant status matters in a cyber conflict with global reach but tangible domestic impact. It also means that some military lawyers, whose area of expertise may be limited to the law of armed conflict, will need to become much better acquainted with the impact *jus ad bellum*, international human rights law and domestic law have on cyber operations. At a minimum, it will present a daunting educational, training and doctrinal challenge for many military and civilian government legal advisors.

B. An "Armed" Attack: Really?

1. Cyber Weapons and Effects

Notwithstanding the requirement to come to grips with the breadth of civilian participation in cyber operations, perhaps the greatest challenge for international lawyers will be to identify when cyber attacks reach the threshold necessary for a State to legitimately respond in self-defense.[71]

---

70. *See* Headquarters, Department of the Army, FM 1-04, Legal Support to the Operational Army ¶ 5-4 (2012) (Operational law is "the body of domestic, foreign, and international law that directly affects the conduct of military operations."); *see also* Office of the Judge Advocate General, Roles and Responsibilities (2012) (defining "operational law" as "that body of domestic and international law that applies to the conduct of all phases of a CF operation at all levels of command").

71. UN Charter art. 51.

With international law indicating "it will be necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms" the international legal community has struggled with identifying the gravity threshold.[72] The mining of a warship might meet that threshold,[73] but mere frontier incidents would not.[74] Given this lack of consensus regarding kinetic uses of force, it is likely cyber attacks will present an even greater challenge.

To even begin to address that issue, there first must be an understanding that a computer is potentially a weapon. In a legal context, a weapon is assessed both as a means and method of warfare that is of a nature to cause superfluous injury or unnecessary suffering.[75] However, the nature of the challenge is perhaps most clearly framed in non-legal terms. A weapon has been defined as: "a thing designed or used for inflicting bodily harm or physical damage: *nuclear weapons*."[76]

This concept of weapon creates two challenges in the cyber domain. The first is the need to convince the broader public that computers (the laptops, desktops, tablets and even phones carried by much of the public, including, no doubt, committed pacifists) are, in fact, weapons like rifles, artillery and fighter aircraft. Of course, as was tragically demonstrated during the genocide in Rwanda, even basic implements such as knives and machetes can be turned into an instrument of mass death.[77] However, the issue is whether the ubiquitous computer, which requires a certain level of sophistication to operate, but does not project a shell or offer much in the way of being a blunt instrument, could also be used as a weapon in its own right.

---

72. Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 191 (June 27) [hereinafter *Nicaragua*].

73. Oil Platforms (Iran v. U.S.), 2003 I.C.J. 161, ¶ 72 (Nov. 6) ("The Court does not exclude the possibility that the mining of a single military vessel might be sufficient to bring into play the 'inherent right of self-defence'. . . ."); *See also* Waxman, *supra* note 44, at 438 (indicating the United States argued successfully for a low Article 51 threshold.).

74. *Nicaragua*, supra note 71, ¶ 194.

75. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 37, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

76. OXFORD DICTIONARIES ONLINE, *supra* note 12 (emphasis added).

77. SAMANTHA POWER, "A PROBLEM FROM HELL": AMERICA AND THE AGE OF GENOCIDE 334 (2002) (outlining how the genocide started with the use of firearms, but as it spread throughout Rwanda the weapons became "increasingly unsophisticated—knives, machetes, spears and the traditional masu, bulky clubs with nails protruding from them").

Second, there must be an acceptance that cyber means can inflict bodily harm or physical damage. This is an area where determining the *lex lata* (what the law is) for the *jus ad bellum* has been particularly challenging. It has led to efforts to assess the "effects" generated by a computer by an analogy to kinetic weapons. Among the questions being debated is whether computer attacks should be looked at using an instrument-based approach (i.e., one that produces equivalent results to a kinetics-based attack) in assessing whether such an attack can reach the level of an armed attack under Article 51 of the UN Charter.[78] However, the conceptual and legal path connecting the pressing of a computer key to ultimately causing a destructive effect approaching that of an armed attack is anything but straightforward. It might be analogized to the bombing of a dam gate thereby releasing floodwaters. As the Stuxnet attack has demonstrated, physical damage can occur. That is not the only way that cyber operations can lead to physical damage, death or injury. For example, a cyber penetration of a SCADA system could be considered the same as a covert insertion of a Special Forces team, which, after gaining access to the control facility, turns the dial opening the gates. While such activity might constitute an armed attack, the overall analysis would benefit by not jumping to a bullets and bombs (i.e., kinetic) approach.[79]

Another method for considering what constitutes an armed attack is the effects-based approach, i.e., whether it produces severe enough effects that it warrants treatment as an armed attack. Jeffrey Carr provides the example of an armed attack in which one party "manipulated information across a state's banking and financial institutions to seriously disrupt commerce in the state."[80] This approach does not try to equate the use of cyber

---

78. An instrument-based approach is described as

> a cyber attack used to shut down a power grid is an armed attack. This is because shutting down a power grid typically required dropping a bomb on a power station or some other kinetic use of force to incapacitate the grid. Since conventional munitions were previously required to achieve the result, under the instrument-based approach the cyber attack is therefore treated the same way.

CARR, *supra* note 1, at 59

79. YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 212 (5th ed. 2011) ("If CNA [computer network attack] were to cause severe damage to property or even human fatalities (as a result, e.g., of the shutdown of computers controlling waterworks and damns, leading to the flooding of inhabited areas), it would qualify as an armed attack.").

80. An effects-based approach is described as

to a kinetic attack, but rather seeks to assess the quantum of loss in an economic sense. The challenge here is twofold. First, as has been noted, international law has struggled with the very notion of categorizing loss in a kinetic context. It is not clear how this approach will add any greater clarity. Second, the effects-based approach appears to involve a particularly commercial calculus.

It is not clear where the separation is between loss, damage, disruption, theft and simple espionage with regard to the ability to conduct commerce. Further, given the nature of international commercial relations, it is not clear whether this approach only involves attacks on nationally owned or based corporations, international corporations and their subsidiaries, private financial institutions, e.g., Wall Street, or institutions more closely associated with the State, such as the Federal Reserve in the United States.

What this approach does do is highlight that the basis for an armed attack has always included an economic component. For example, the establishment of a blockade by one State against another, albeit with the threat of military force backing it, could be seen as an armed attack justifying a response in self-defense.[81] It is not clear, however, that the likely means of a cyber blockade, a DDoS attack, even falls under the effects-based approach or equates to a use of force under Article 2(4) of the Charter? It must constitute a use of force before it can be considered as an armed attack.

This raises the question of whether the use of force under Article 2(4) is broader than simply armed force extended to economic matters. Such an interpretation is one that most Western economically powerful States and international lawyers have resisted, although "developing countries and formerly the Eastern bloc countries have repeatedly claimed that the prohibition on the use of force also comprises other forms of force, for instance, political and, in particular, economic coercion."[82]

> a cyber attack that manipulated information across a state's banking and financial institutions to seriously disrupt commerce in the state is an armed attack. Although the manipulation of information does not resemble a kinetic attack, as required under an instrument-based approach, the disruptive effects that the attack had on the state's economy is a severe enough overall consequence that it warrants treatment as an armed attack.

CARR, *supra* note 1, at 59

81. Albrecht Randelzhofer, *Article 51*, *in* 1 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 788, 797 (Bruno Simma ed., 2d ed. 2002).

82. Albrecht Randelzhofer, *Article 2(4)*, *in id.* at 112, 118. *See also* CHRISTINE GRAY, INTERNATIONAL LAW AND THE USE OF FORCE 30 (3d ed., 2008) ("There is a split be-

Malcolm Shaw notes this issue was considered in the past in "light of the Arab oil weapon used in 1973-4 against States deemed favorable to Israel."[83] While he indicates there is a case to be made that such actions are contrary to the Charter, ultimately "whether such action constitutes a violation of Article 2(4) is dubious."[84] The prevailing view is that economic coercion would not qualify as a use of force under Article 2(4), let alone form the justification for acting in self-defense under Article 51.[85] In this respect it has been noted, "were this provision [Article 2(4)] to extend to other forms of force, States would be left with no means of exerting pressure on other States that violate the law."[86] This is an important issue when considering the use of cyber means in the form of countermeasures.

Given this background, an effort by economically powerful States, such as the United States, that have computer-based economies to now widen the basis for reaction in self-defense by including the economic impact of computer activity as an armed attack could have unintended consequences if it results in a broadening of Article 2(4) to include economic coercion. This is not to suggest it should not be done, but in doing so a careful analysis needs to be undertaken that looks beyond the narrow interests of the more technologically advanced States. At the same time, it would also be ironic if less economically developed States, which might also have less advanced cyber capabilities, embraced an argument that such "economic" focused uses of cyber were not an armed attack under international law because of the asymmetric advantage they now might have.

---

tween developed and developing states as to whether 'the use of force' includes not only armed force but economic coercion."); Waxman, *supra* note 44, at 428–29.

83. SHAW, *supra* note 32, at 1125. *See also* Michael N. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, 37 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 885 (1999), *reprinted in* ESSAYS ON LAW AND WAR AT THE FAULT LINES 3, 24 (Michael N. Schmitt ed., 2012) ("Because the results of applying economic and political instruments constitute lesser threats to shared community values, the use of force standard serves as a logical break point in categorizing the asperity of particular coercive acts.").

84. SHAW, *supra* note 32, at 1125.

85. *See* DINSTEIN, *supra* note 79, at 88 ("[W]hen studied in context, the term 'force' in Article 2(4) must denote violence. It does not matter what specific means—kinetic or electronic are used to bring it about, but the end result must be that violence occurs or is threatened. Therefore, psychological or economic pressure (e.g. in the form or economic boycott) as such does not come within the purview of the Article, unless coupled with the use or at least the threat of force."); Schmitt, *supra* note 83, at 22.

86. Randelzofher, *supra* note 82, at 118.

2. Cyber and Force

Of course, even before there is a discussion of armed attack there must be acceptance that there is a use of force.[87] There is an interpretation of the law developed in 1999 by Michael Schmitt that cyber specific criteria, e.g., severity, immediacy, directness, invasiveness, measurability and presumptive legitimacy, could be applied to assess if a use of force has occurred.[88] These criteria appear to fall well within the concept of *lex ferenda*, or what the law ought to be. Indeed, the 2013 *Tallinn Manual*, a project in which this author participated, indicates the criteria are not to be viewed as formal legal requirements, but rather as factors "that influence States making use of force assessments."[89]

Of note, these factors are set out in the *Manual* commentary rather than the rules.[90] In the *Tallinn Manual*, it is stated the rules "reflect consensus among the Experts as to the applicable *lex lata*, that is, the law currently governing cyber conflict. It does not set forth *lex ferenda,* best practice, or preferred policy."[91] The commentary is "intended to identify its legal basis, explain its normative content, address practical implications in the cyber context, and set forth differing positions as to scope or interpretation."[92] The fact that the *lex lata* in this instance is justified by such extensive reference to relatively recent interpretations of the law, even if it was only in the context of taking note of the theory, stands out as an example of the challenge presented by cyber warfare.[93] The technology is new, indeed cutting

87. For an excellent discussion of Article 2(4) in the cyber context, see Waxman, *supra* note 44.

88. Schmitt, *supra* note 83, at 26.

89. TALLINN MANUAL, *supra* note 4, rule 11, ¶ 9.

90. *Id.*, rule 11, ¶¶ 8–11.

91. *Id.* at 19.

92. *Id.* at 20.

93. The *Tallinn Manual* explains the rationale for using these criteria as follows:

> Acts that injure or kill persons or damage or destroy objects are unambiguously uses of force (see commentary to Rule 13 expressing an analogous conclusion, but requiring the harm to be 'significant'). Since other cases are less clear, the International Group of Experts took notice of an approach that seeks to assess the likelihood that States will characterise a cyber operation as a use of force. The method expounded operates on the premise that in the absence of a conclusive definitional threshold, States contemplating cyber operations, or that are the target thereof, must be highly sensitive to the international community's probable assessment of whether the operations violate the prohibition on the use of force.

edge, but the established law is "old" law, which is, in many ways, retrospective to the immediate post-World War II era.

What adopting these factors would mean is an acceptance of a dual threshold for assessing force and cyber operations. In this respect, the *Tallinn Manual* indicates "[a] cyber operation constitutes a use of force when its *scale and effects* are comparable to non-cyber operations rising to the level of a use of force."[94] Similarly, "[w]hether a cyber operation constitutes an armed attack depends on its *scale and effects*."[95] The *Manual* relies on the same interpretation of the *Nicaragua* decision to explain the use of the term "scale and effect" as the basis for assessing both the use of force[96] and armed attack.[97] However, "[t]he scale and effects required for an act to be characterised as an armed attack necessarily exceed those qualifying the act as a use of force."[98]

While this is a sound interpretation of widely accepted principles of international law as it has developed to date, it is not clear how well this standard will be applied in practice. A majority of the experts writing the *Manual* were reported to have believed "the critical factor was whether the effects of a cyber operation, as distinct from the means used to achieve those effects, were analogous to those that would result from an action otherwise qualifying as a kinetic armed attack."[99] This suggests an instruments-based approach, although the scale-and-effects argument arguably fits more comfortably with the effects-based approach. There is a degree of overlap between both approaches in that one of the factors that often points to a kinetic armed attack is the tangibly measurable effects created by that violence.

The instruments-based approach appears to be the one favored by the United States Government for assessing if a use of force has occurred. As was indicated by the U.S. State Department Legal Advisor Harold Koh in September 2012, "if the physical consequences of a cyber attack work the kind of physical damage that dropping a bomb or firing a missile would,

---

Id., rule 11, ¶ 8 (citation omitted).
94. *Id.*, rule 11 (emphasis added).
95. *Id.*, rule 13 (emphasis added).
96. *Id.*, rule 11, ¶ 1.
97. *Id.,* rule 13, ¶ 6.
98. *Id.,* rule 13, ¶ 5.
99. *Id.,* rule 13, ¶ 4.

that cyber attack should equally be considered a use of force."[100] Of note, these references were made with respect to meeting the basic threshold of a use of force. Mr. Koh also reiterated the United States' position that "there is no threshold for a use of deadly force to qualify as an 'armed attack' that may warrant a forcible response."[101] While this continues to place the United States in an outlier position in relation to the broader international community regarding the legal basis for acting in self-defense, there is little chance that a cyber context would have changed this approach given the general lack of consensus regarding what constitutes a use of force in that domain. That said, the United States, or any other State that takes this position, will still need to identify the threshold for a use of force at which point a response in self-defense would be justified.

Further, it is not clear if any message can be taken from the fact that the examples provided—the causing of a nuclear plant meltdown, opening dam doors and disabling air traffic control—did not include an attack on the financial markets.[102] Its omission may simply reflect what conceptually difficult issues such an attack poses for traditional international law. These examples also do not clearly establish the minimum threshold upon which action is considered justified. Further, it was noted that "there are other types of cyber actions that do not have a clear kinetic parallel, which raise profound questions about exactly what we mean by 'force.'"[103]

The *Tallinn Manual* does address attacks on financial institutions; however, the commentary discussion of what is described as the "classic scenario" of an attack on the New York Stock Exchange reflected quite divided opinions that go to the heart of the discussion of regulating force in the cyber domain.[104] There is a danger that the reference to the New York Stock Exchange shows a Western and, in particular, U.S. concern with interference with commerce. An interesting issue is whether disruption of the

---

100. Harold Koh, Legal Advisor, U.S. Department of State, Remarks at USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), *available at* http://www.state.gov/s/l/ releases/remarks/197924.htm [hereinafter *Koh Remarks*].

101. *Id. See also* Sean D. Murphy, *U.S. Reaction to ICJ Judgment in Iranian Oil Platforms Case*, 98 AMERICAN JOURNAL OF INTERNATIONAL LAW 597 (2004).

102. *Koh Remarks*, *supra* note 100.

103. *Id.*

104. TALLINN MANUAL, *supra* note 4, rule 13, ¶ 9 ("Some of the Experts took the position that harm to persons or physical damage to property is a condition precedent to the characterisation of an incident as an armed attack. Others took the view that it is not the nature (injurious or destructive) of the consequences that matters, but rather the extent of the ensuing effects.").

Shanghai, Tokyo or London stock exchanges would garner the same concerns. Further, given the interconnected nature of the financial markets, if there was an attack on one of these other exchanges could another State claim it was an attack on their economic interests, if they were adversely impacted collaterally, even though the State hosting the targeted exchange did not share the view? This lack of consensus and the unclear theoretical underpinning for such activity to be called an armed attack suggests caution is required in coming to any conclusions at this stage.

There is a significant danger in overstating the effects of cyber attacks even when they impact on infrastructure such as dams, power generation facilities or other utilities. Again it may be helpful to return to the Y2K experience. Notwithstanding dire predictions regarding potential failures of SCADA and other computerized systems controlling pipelines, electrical grids, trains and even weapon systems,[105] a study of many of these systems at the time of Y2K demonstrated they were quite resilient. As the *United States Y2K Study* indicated, critical industries "include a great deal of competing systems created by deregulation and technological advancements in recent decades."[106] A particular exception was the electrical power distribution network; however, even here there was substantial redundancy.[107] As that study noted in its discussion of critical infrastructure, "[i]n an economy as large as the United States, hundreds and perhaps thousands of failures in 'critical infrastructure' electricity or water systems could occur before the impact would be great enough before there would be a significant impact."[108]

Another challenge in assessing the impact of cyber operations is that the infrastructure itself may be particularly vulnerable to being adversely affected by other factors unrelated to the intensity of the cyber activity. In other words a piece of malware may not, on its own, be a use of force or an attack, although its presence may have unintended consequences. It is reported that in 2003, fifty million people were out of power in the eastern United States and central Canada because a falling tree created a surge in a power line that apparently slowed back up controls, in part, because of a software glitch and computer malware.[109] In situations such as this, sorting out the responsibility for the actual blackout may be difficult to ascertain.

105. CLARKE & KNAKE, *supra* note 14, at 96–101.
106. *United States Y2K Study*, *supra* note 15, at 23.
107. *Id.*
108. *Id.* at 7.
109. CLARKE & KNAKE, *supra* note14, at 99.

One challenge appears to be the relative reliability and robustness of the power grid. For example, a former Energy Secretary in the United States noted notwithstanding U.S. military and economic might has

> a grid that is antiquated, that is Third World, that needs beefing up. We've got very weak power transmission lines and generation capacity. That's because there hasn't been investment in our electricity grid because there's been no competition, because there's been a lot of monopoly control of utilities in this country.[110]

Not only does there need to be further study to gather the facts, the legal community should reach out to other disciplines to become better informed before embracing the notion that a cyber-induced power failure generally provides the threshold for the existence of an armed attack.

Another factor to be considered in assessing the scale and effects of cyber operations is that many populations have shown themselves to be quite resilient when confronted with either man-made or natural disasters. This has included significant power failures or blackouts affecting millions of persons both within a country and extending across borders. In addition to the above-mentioned 2003 North American incident, significant blackouts have occurred in Europe in 2006[111] and more recently in India in 2012.[112] Some disruptions have occurred in inhospitable climates, such as in Canada as a result of an ice storm during the winter of 1998[113] and in the

---

110. Interview with Bill Richardson, former U.S. Secretary of Energy, Frontline, PBS (Apr. 10,2001), http://www.pbs.org/wgbh/pages/frontline/shows/blackout/interviews/richardson.html.

111. Stephen Castle, *Europe suffers worst blackout for three decades*, THE INDEPENDENT (Nov. 6, 2006), http://www.independent.co.uk/news/world/europe/europe-suffers-worst-blackout-for-three-decades-423144.html# ("The power loss came about when Germany's network became overloaded, probably as a result of a routine shut down of a high-voltage transmission line under the Ems river to allow a ship to pass by safely. The fallout from the incident, said to be one of the worst since the 1970s, left engineers and politicians aghast, and underlined the interdependence of European countries' electricity grids.").

112. *India blackouts affect half the country*, CBC NEWS (July 31, 2012), http://www.cbc.ca/news/world/story/2012/07/31/india-power-outage.html ("Its impact, however, was softened by Indians' familiarity with frequent blackouts and the widespread use of backup generators for major businesses and key facilities such as hospitals and airports.").

113. Eric Harris, *Struck Powerless*, CANADIAN GEOGRAPHIC, Mar.–Apr. 1998, *available at* http://www.canadiangeographic.ca/magazine/ma98/feature_ice_storm.asp.

United States in 2009.[114] Given that States deal with these types of challenges on a fairly regular basis, this may inoculate their societies from rushing to a conclusion that cyber events leading to SCADA interference should be viewed as such a threat to national security that going to war is warranted.

As a result, to take the position that cyber activity causing a power failure generally establishes the threshold for an armed attack, or even constitutes a use of force permitting an armed response if the United States position is applied, could be problematic. Without developing a generally agreed to scale-and-effects assessment of the actual, or even potential, impact of such cyber activity a State could embark down a course leading to an armed conflict involving not only wider cyber attacks, but also kinetic violence.

It may be that the international law standard of a grave use of force justifying action in self-defense may not readily translate in equivalency to the effects of a power failure that is not exceptionally disruptive to the overall functioning of the economy of a State, or cause a substantial loss of life.[115] The question from an *ad bellum* perspective is at what point effects that can also be caused by human frailty or weather should be equated to an armed attack, such that they justifiably prompt a response that could result in two or more nations going to war.

That is not to say that interference with SCADA systems could not reach the threshold of an armed attack if you apply a scale-and-effects approach. Not all cyber-induced failures of power and other industries would necessarily reach that threshold, however. Indeed, there is some skepticism that a purely cyber war will ever develop that would be "violent, instrumental, and—most importantly—politically attributed."[116]

---

114. *See Ice Storm Cuts Power Throughout Northeast*, CBS NEWS (Feb. 11, 2009), http://www.cbsnews.com/2100-201_162-4665303.html.

115. CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 4, at 119 (referencing an advisor report for the Dutch government that indicated that where there is a cyber attack to leading to "a *significant* number of fatalities or causes *substantial* physical damage or destruction to vital infrastructure, military platforms or installations or civil property, it could certainly be qualified as an 'armed attack'") (emphasis added).

116. Thomas Rid, *Cyber War Will Not Take Place*, 35 JOURNAL OF STRATEGIC STUDIES 5, 29 (2012).

3. Countermeasures

A real advantage of cyber operations is that much of the activity occurs outside of the public eye at a micro level not normally associated with armed conflict. This presents two types of opportunities for a State. One is to covertly engage in activity that reaches the level of a use of force or an armed attack and rely on such activity not being discovered or attributed to that State.[117] Such activity is problematic from an international law perspective. Another advantage of this new technology is that it provides a means for a State to act in response to threats without crossing the armed conflict threshold. In effect, it is one of the means by which wider and more violent conflict can be avoided in the first place. When the cyber activity amounts to an internationally wrongful act, there are options short of war for responding to threats under the international legal system. The problem is that those responses are often excluded—or at least pushed into the background—in the contemporary dialogue regarding operations in the cyber domain which appears to focus on force.

There is the very real danger that focusing discussion on the less likely occurrence of armed attack will overshadow the potential use of cyber in other circumstances. In this regard a cyber weapon might be thought of in less bellicose terms by considering it in the context of the rest of the Oxford definition: "a means of gaining an advantage or defending oneself in a conflict or contest: *resignation threats had long been a weapon in his armoury*."[118]

Perhaps a primary function of cyber is more accurately considered as a weapon of a different sort, one divorced from those producing kinetic results. Cyber should not necessarily be seen as having a violence-producing capability at the level of an armed attack—or even a use of armed force. Instead, it is simply a use of force, or maybe not even that. Cyber activities have the potential to offer a non-violent means to sanction a State for its internationally wrongful act as countermeasures.[119]

---

117. Arquilla, *supra* note 42 ("The culprit is the bits and bytes that are the principal weapons of cyberwar. It is now possible to intervene swiftly and secretly anywhere in the world, riding the rails of the global information infrastructure to strike at one's enemies. Such attacks can be mounted with little risk of discovery, as the veil of anonymity that cloaks the virtual domain is hard to pierce. And even when 'outed,' a lack of convincing forensic evidence to finger the perpetrator makes heated denials hard to disprove.").

118. OXFORD DICTIONARIES ONLINE, *supra* note 12 (emphasis added).

119. *Nicaragua, supra* note 71, at 106, ¶ 201 ("[T]he Court must enquire whether there is any justification for the activities in question, to be found not in the right of collective

The *Tallinn Manual* addresses countermeasures in Rule 9, which states "[a] State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State."[120] A widely held view is that countermeasures cannot involve the use of armed force.[121] Countermeasures are exceptional in that they may justify otherwise unlawful conduct taken in response to a previous intentionally wrongful act of another State.[122] In this respect, they are different than retorsion, which is a response by means of an "unfriendly act not amounting to a violation of international law, to either (a) a breach of international law or (b) an unfriendly act, by another State."[123] Retorsion can include breaking off diplomatic relations, discontinuing or withholding of trade, denying economic or financial benefits, etc.[124] Importantly, acts of retorsion can involve cyber measures, such as occurred when Estonia "suspended some services to internet protocol (IP) addresses from Russia."[125]

The concept of countermeasures is a broad one with reference sometimes being "made to the application of a 'sanction' or to a 'reaction' to a prior internationally wrongful act; historically the more usual terminology was that of 'legitimate reprisals' or, more generally, measures of 'self-protection' or 'self-help.'"[126] Countermeasures "are essentially temporary measures, taken to achieve a specified end, whose justification terminates once the end is achieved."[127] The wide range of permissible non-forcible actions is reflected, in part, in Article 41 of the UN Charter in its reference to "measures not involving the use of armed force," including "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of

---

self-defence against an armed attack, but in the right to take counter-measures in response to conduct of Nicaragua which is not alleged to constitute an armed attack.").

120. TALLINN MANUAL, *supra* note 4, rule 9.

121. *See* DINSTEIN, *supra* note 79, at 209.

122. Draft Articles on Responsibility of States for Internationally Wrongful Acts art. 22, ¶ (2), at 75, Rep. of the Int'l L. Comm'n, 53d Sess., UN GAOR 56th Sess., Supp. No. 10, at 181, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 26, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2), *available at* http://untreaty.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [hereinafter *Draft Articles on State Responsibility*]

123. ANTONIO CASSESE, INTERNATIONAL LAW 310 (2d ed. 2005).

124. *Id.*

125. TALLINN MANUAL, *supra* note 4, rule 9, ¶ 13.

126. *Draft Articles on State Responsibility*, *supra* note 122, art. 22, ¶ (3), at 75.

127. *Id.*, ch. II cmt. ¶ (4), at 129.

diplomatic relations." This article specifically endorses economic coercion, although only when decided by the Security Council.[128] That being said, these measures are reflective of the types of countermeasures and acts of retorsion that might be contemplated since they are viewed as not involving the use of armed force.

The reference to measures involving economic coercion further highlights that rushing too quickly to include the disruption of commerce under the scope of a cyber armed attack may actually restrict policy and operational options available to technologically advanced States. Those States must, however, be prepared to confront a more level cyber playing field with traditionally less capable States, which respond to advanced State activities by interfering with their economies. Economically powerful States might, however, have a very low threshold of acceptance for such activity.

The debate over cyber countermeasures may also cause a reconsideration of whether such measures can involve the use of force that falls below the level of armed attack. Judge Simma, in his separate opinion in the *Oil Platforms* case, concluded that countermeasures "[a]gainst such smaller scale use[s] of force, defensive action—by force also 'short of' Article 51—is to be regarded as lawful."[129] Such an approach garnered the support of other respected academics, although this view of the law has remained a minority one.[130] However, it may be preferable to allow more limited cyber exchanges between potential antagonists than force the confrontation into the realm of self-defense and ultimately armed conflict. The challenge when using computer network operations as a countermeasure is to ensure that the response remains below the threshold of an armed attack. This requires an ability to identify and articulate where on the gravity scale such a cyber use of armed force will lie, which has proven difficult to identify.[131] The

128. W. MICHAEL REISMAN & JAMES E. BAKER, REGULATING COVERT ACTION 28 (1992).

129. *See* Oil Platforms*, supra* note 73, at 332, ¶ 12 (separate opinion of Judge Simma).

130. *See* CASSESE, *supra* note 123, at 371–72; THOMAS M. FRANCK, RECOURSE TO FORCE: STATE ACTION AGAINST THREATS AND ARMED ATTACKS 109–112 (2002) (recognizing the right to use force measures in response to attacks below the threshold of "armed attack."). *But see* LINDSAY MOIR, REAPPRAISING THE RESORT TO FORCE: INTERNATIONAL LAW, *JUS AD BELLUM* AND THE WAR ON TERROR 29 (2010) (noting that other commentators have taken the view "any such activities were violations of the *jus ad bellum*").

131. *See* REISMAN & BAKER, *supra* note 128, at 28 (noting that the language of some United Nations resolutions "prohibits only grave forms of coercion without indicating

legal assessment of the gravity of an attack has not been made any easier by the terminology that is commonly employed with respect to such cyber activity. It is that issue to which the analysis will now turn.

4. Terminology: The Impact of Words

It may very well be that the dialogue of cyber is pushed into the force realm by the terminology that has been applied to describe cyber activity. The most obvious examples are the terms "computer network *attack*"[132] and "computer network *defense*."[133] However, it is also evident in the national cyber security policy of Canada, which extends the concept of cyber attack to unintentional access to and use of information.[134] The use of the term "attack" invokes a perception of military activity, but in reality the cyber activity may simply involve limited manipulation of information.

A downside of lawyers entering the cyber highway so late is that there has not been an opportunity to help select the terms used to describe cyber operations. While the operational, doctrinal and legal communities use the same words, those words do not always have the same meaning. The use of the warlike term "attack" for an exceptionally broad range of computer activity is fraught with the potential for misunderstanding and overreaction that can have significant consequences, particularly at a strategic level. A political leader or media outlet may rightly claim, from a doctrinal perspective, that a "computer network attack" has taken place when another State is alleged to have hacked into the data-storage system and stolen sensitive

---

where and how minor economic coercion becomes grave"). *See also* Waxman, *supra* note 44, at 429.

132. "Computer network attack" is defined as "[a]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA." Joint Chiefs of Staff, Joint Publication 1-02, DOD Dictionary of Military and Associated Terms (Nov. 8, 2010), as amended through July 15, 2012, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

133. "Computer network defense" is defined as "[a]ctions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks. Also called CND." *Id.*

134. *Canada's Cyber Security Strategy*, *supra* note 45, at 3 ("Cyber attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security.").

information relating to a defense procurement project.[135] That statement could create the perception that there was an act of force inflicted by one State on another, when the "attack" simply involved the destruction of information on a computer or was conducted as a step precedent to an act of espionage. The real challenge for many States is that they are themselves engaged in the same activity.[136] Calling such activity an attack could make it easier for other States to characterize what is, in effect, espionage as illegitimate. This could be exceptionally counterproductive for the State subjected to the espionage when the issue is assessed from a broader strategic perspective.[137]

The gap in meaning between a computer network attack and even the low threshold of a use of force under the *jus ad bellum* highlights the risks inherent in not adopting a commonly acceptable language to describe activities in the cyber domain. Significantly, the use of terms like attack also potentially limits non-forceful responses, since even the most basic penetration of a computer network appears to engage some aspect of computer network attack. For example, a State may be reluctant to use cyber means to respond to incidents out of concern relatively minor cyber activity can be mischaracterized as a more aggressive action potentially justifying a kinetic response by the aggrieved State.

There is terminology from the criminal sphere, such as "illegal access," "illegal interception," "data interference," "misuse of devices," "computer related forgery" and "computer related fraud" found in the Council of Europe's Convention on Cybercrime that may more clearly define most cyber activity and provide less opportunity for misunderstanding and confusion.[138] It is noteworthy that the use of terms such as attack was avoided in the convention, although attacks are referred to in its accompanying ex-

135. CLARKE & KNAKE, *supra* note 14, at 233–35.

136. *Id.* at 235 ("The ways in which we collect information, including by cyber espionage, may offend some people's sensibilities and may sometimes violate international or national laws, but, with some notable exceptions, U.S. espionage activities are generally necessary and beneficial to U.S. interests.").

137. *Id.* (noting that even entering into a treaty to limit such activity would be problematic from a national security perspective).

138. Council of Europe, Convention on Cybercrime arts. 2–6, Nov. 21, 2001, E.T.S. 185, *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm; Paul A. Matus, *Strategic Impact of Cyber Warfare Rules for the United States* 10–13, 31–2 (2010), *available at* http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA522001

planatory report.[139] What is not clear is how easy it would be at this stage to alter the attack terminology that may have become entrenched in national security doctrine. But the use of terms focused on criminal activity, when that in fact is what is being described in such doctrine, would help avoid confusion and misunderstanding regarding the nature of the cyber threat from a national defense perspective.

In many respects, terminology in the non-legal world has shown itself to be more subject to change than its legal counterpart. Perhaps one of the best examples of the fluidity of terminology can be found in the efforts to describe guerrilla warfare. In this regard, a myriad of terms have been applied to such conflicts, including "small wars,"[140] "imperial policing,"[141] "police action,"[142] "insurgency,"[143] low intensity conflict,"[144] "military operations other than war,"[145] "peacekeeping,"[146] "peace enforcement,"[147] three

139. Council of Europe, Committee of Ministers, Convention on Cybercrime, Explanatory Report (Nov. 8, 2001), *available at* http://conventions.coe.int/Treaty/en/Reports/Html/185.htm .

140. *See* C.E. CALDWELL, SMALL WARS: THEIR PRINCIPLES AND PRACTICE 21 (3d ed. 1996); MAX BOOT, THE SAVAGE WARS OF PEACE: SMALL WARS AND THE RISE OF AMERICAN POWER xiv (2002).

141. *See* MAJOR-GENERAL SIR CHARLES W. GWYNN, IMPERIAL POLICING 3–4 (1934).

142. *See* Josef L. Kunz, *The Chaotic Status of the Laws of War and the Urgent Necessity for Their Revision,* 45 AMERICAN JOURNAL OF INTERNATIONAL LAW 37, 54 n.41 (1951) (citing P.C. Jessup, A MODERN LAW OF NATIONS 188–89 (1948) ("It is a mistake to assume that the acceptance of the concept of an international police force . . . with its subsequent abolition of the concept of 'war' in a legal sense, eliminates the necessity for the legal regulation of the rights and duties of those who are active participants in the struggle.").

143. *See* Headquarters, Departments of the Army and Air Force, FM 100-20/AFP 3-20 Military Operations in Low Intensity Conflict (1990), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB63/doc4.pdf (superseded by FM 3-07 (2003), which in turn was replaced in 2008).

144. *Id.*

145. *See* Headquarters, Department of the Army, FM 3-07 (FM 100-20), Stability Operations and Support Operations 1-1 (2003), *available at* http://usacac.army.mil/cac2/cgsc/carl/docrepository/fm3_07.pdf.

146. *See* DEPARTMENT OF PEACEKEEPING OPERATIONS, UNITED NATIONS PEACEKEEPING OPERATIONS: PRINCIPLES AND GUIDELINES 17 (2008), *available at* http://pbpu.unlb.org/pbps/library/capstone_doctrine_eNg.pdf (noting where the spectrum of peace and security activities is identified as conflict prevention, peacemaking, peacekeeping, peace enforcement and peace building).

147. *Id.*

block war,"[148] "revolutionary warfare,"[149] "irregular warfare,"[150] "war amongst the people,"[151] "mosaic war"[152] and "hybrid warfare."[153] One of the strengths of the legal approach, although also a potential weakness in terms of addressing new technology, has been its more consistent use of terminology. State legal advisors would likely have to present a convincing argument that terminology has to be changed. In this regard, they may be assisted if non-lawyers pause to think of the operational flexibility at the strategic level that the use of less warlike terms can offer.

IV. THE ROAD AHEAD

It is evident the cyber domain presents significant new challenges for interpreters of the *jus ad bellum*. A key issue to be addressed is the willingness of the international legal community to accept change to long-standing interpretations of the use of force under that body of law. For those lawyers who work for government, human rights advocates and academics, serious questions need to be asked—and answered—as to whether there is a need to create a whole new terminology and new principles regarding the use of cyber. This will present a daunting challenge for some parts of the international legal community who, even now, more than a decade after 9/11, either do not recognize[154] or only give grudging acceptance to the Security Council's determination that the right of self-defense under Article 51 can

148. *See* Charles C. Krulak, *The Strategic Corporal: Leadership in the Three Block War*, MARINES MAGAZINE, Jan. 1999, at 3, *available at* http://www.au.af.mil/au/awc/awcgate/usmc/strategic_corporal.htm.

149. *See* Bernard B. Fall, *The Theory and Practice of Insurgency and Counterinsurgency,* NAVAL WAR COLLEGE REVIEW, Winter 1998, at 46, 47.

150. *See* Kenneth C. Coons Jr. & Glenn M. Harned, *Irregular Warfare Is Warfare*, 52 JOINT FORCES QUARTERLY, Jan. 2009, at 97.

151. *See* GENERAL SIR RUPERT SMITH, THE UTILITY OF FORCE: THE ART OF WAR IN THE MODERN WORLD 3–4 (2007).

152. *See* Headquarters, Department of the Army & Headquarters, Marine Corps Combat Development Command, FM3-24/MCWP 3-33.5, Counterinsurgency ¶ 1–37 (2006).

153. DAVID KILCULLEN, THE ACCIDENTAL GUERRILLA: FIGHTING SMALL WARS IN THE MIDST OF A BIG ONE 4 (2009).

154. Randelzhofer, *supra* note 81, at 802 ("Acts of terrorism committed by private groups or organizations as such are not armed attacks in the meaning of Art. 51 of the UN Charter. But if large scale acts of terrorism of private groups are attributable to a State, they are an armed attack in the sense of Art. 51.").

be exercised against non-State actors who are not associated with a State.[155] As an initial foray into assessing cyber warfare in this context, the *Tallinn Manual* does not indicate that the necessary consensus will be easily reached on such a foundational issue. After reviewing what it describes as a controversial topic, it states "[s]uch State practice *appears* to signal a *willingness* of States to apply the right of self-defense to attacks conducted by non-State actors."[156] There is a very real danger that advances in technology are outstripping the pace of the legal dialogue.

It can only be hoped that more success is attained in clarifying the law surrounding the cyber domain than appears to have been the case with direct participation in hostilities. More than a decade after targeted killings attracted the attention of the international legal community, there still appears to be a lack of consensus on who qualifies as a lawful target. This is the case with regard to the question of whether members of organized armed groups can be targeted by virtue of their membership and, if so, how such membership is determined.[157] It was also noted in 2012 that "there is a range of views among the United States and its partners on the precise 'test' that should be applied to determine membership."[158] This is an area where the responsibility rests primarily with States, however, the State approach to defining that term still appears to be shrouded in a fog of ambiguity.

---

155. GRAY, *supra* note 82, at 198 (noting the reaction by states to the 9/11 attacks "may be seen as raising the question whether there has been a significant change in the law"). *But see* MOIR, *supra* note 129, at 51 ("[I]t would be extremely difficult to insist that the events of 11 September 2001 did not, and—in international law—*could not*, amount to an armed attack on the United States.") (emphasis added).

156. TALLINN MANUAL, *supra* note 4, rule 13, ¶ 16 (emphasis added).

157. Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions,

Study on Targeted Killings ¶ 65, Human Rights Council, U.N. Doc. A/HRC/14/24/Add.6 (May 28, 2010) (by Philip Alston),(2010), *available at* http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf ("In its general approach to DPH, the ICRC is correct to focus on function (the kind of act) rather than status (combatant vs. unprivileged belligerent) [of organized armed groups], but the creation of CCF [continuous combat function] category is, *de facto*, a status determination that is questionable given the specific treaty language that limits direct participation to 'for such time' as opposed to 'all the time.'").

158. Stephen Pomper*, Toward a Limited Consensus on the Loss of Civilian Immunity in Non-International Armed Conflict: Making Progress through Practice*, 88 NON-INTERNATIONAL ARMED CONFLICT IN THE TWENTY-FIRST CENTURY 181, 188–89 (Kenneth Watkin & Andrew J. Norris eds., 2012) (Vol. 88, U.S. Naval War College International Law Studies).

The fact that DPH is also an important issue for cyber warfare compounds the challenge facing those seeking to provide legal certainty to persons tasked with the responsible application of cyber force. Ambiguity as to how the law applies to cyber warfare has a positive aspect in that it provides operational space as a legal and policy consensus is being developed, while still acknowledging the requirement to operate within a legal envelope. However, the lack of certainty also potentially undermines the establishment of clear accountability "red lines." It can also have an adverse impact on the ability to control the actions of States, which, of course, is the very reason that the modern *jus ad bellum* and *jus in bello* were developed during the twentieth century.

If all of this is a challenge for government lawyers it may a greater one for those working for human rights advocacy groups. Certainly, there are options for human rights advocates to become cyber literate through access to academia and by hiring retired experts. They will also have to undergo a paradigm shift in their thinking, including expanding their horizons beyond the laws in war to the laws governing the recourse to war. Perhaps one of the most interesting aspects of cyber is that it has breathed life into the *jus ad bellum* discipline, which had fallen somewhat into the background of legal discussion given the predominance of non-international armed conflict in the post-Cold War era.[159]

States are testing the boundaries, not only of the technical applications of cyber, but also societal tolerance for its use or abuse. This presents a challenge for technical, operational and legal personnel interested in regulating its use. The information superhighway is becoming increasingly crowded with participants who are being forced to slow down, yield or perhaps even stop some activities. The intervention of lawyers will not always be seen as a positive development.[160] While cyber warfare developers and operators are being required to expose their inventions and capabilities, lawyers are finding themselves having to use nearly seventy-year-old law developed for different circumstances to deal with new technology. For those lawyers both inside and outside of government whose comfort zone

159. JACK S. LEVY & WILLIAM R. THOMPSON, CAUSES OF WAR 12 (2010) ("[T]here has been a shift in the nature of warfare over time—away from the great powers, away from Europe, and, increasingly, away from state-to-state conflict and toward civil war, insurgency, and other forms of intrastate and trans-state warfare.").

160. *See* Stewart Baker, *Denial of Service*, FOREIGN POLICY (Sept. 20, 2011), *available at* http://www.foreignpolicy.com/articles/2011/09/30/denial_of_service.

is "old rules" and "old conflicts," this will be a challenging time as they grapple with new technology and new warfare.

For lawyers embarked on this path to deal with the mankind's latest technological advancement, there is some hope that can be taken from history regarding their ultimate success in establishing a legal framework to govern its operations. Take an example from the *jus in bello* context, such as aerial warfare, where the law of armed conflict has been applied to new technology, in this case operating in "the third dimension."[161] The introduction of air warfare during the twentieth century presented a significant and daunting challenge to the legal community in its efforts to regulate its application during armed conflict. As was evident in the post-World War I debate over airpower, reaching consensus on regulation was difficult, as there were two "opposite tendencies . . . the ideology of extreme pacifists, well intentioned, good but utterly utopian and the thinking of hard and shrewd people . . . who wanted to keep their hands free as to the conduct of the next war."[162] Not only were initial efforts at regulating airpower through the development of the 1923 Hague Rules of Aerial Warfare largely unsuccessful,[163] one view in 1950 was that the use of airpower during World War II had reduced the principle of distinction to a hollow phrase: "in the matter of aerial bombardment there is no rule firmly grounded in the past on which we can place reliance—for aerial bombardment is a new weapon which raises new problems."[164]

It took the concern over wide-scale bombing in World War II, as well as the concerted attention of the human rights community in the 1960s and 1970s, for convention based legal rules for precautions governing targeting to be developed in Additional Protocol I.[165] These rules are now accepted

161. CYBER WARFARE: CRITICAL PERSPECTIVES, *supra* note 4, at 121.

162. Kunz, *supra* note 142, at 39. *See also* DOCUMENTS ON THE LAWS OF WAR 140 (Adam Roberts & Richard Guelff eds., 2005) (explaining that "heightened awareness of the military potential of aircraft was a serious obstacle to reaching agreement").

163. DOCUMENTS ON THE LAWS OF WAR, *supra* note 162, at 139 ("The 1923 Hague Draft Rules were never adopted in legally binding form, but at the time they were regarded as an authoritative attempt to clarify and formulate rules of air warfare, and largely corresponded to customary rules and general principles underlying the laws of war on land and at sea.").

164. Hersh Lauterpacht, *The Problem of the Revision of the Law of War*, 29 BRITISH YEARBOOK OF INTERNATIONAL LAW 360, 364–66 (1952).

165. For an outline of the role in human rights non-governmental organizations in forcing the United Nations to take up the issue of the amendment of international humanitarian law, which led to Additional Protocol I and Additional Protocol II, see KEITH SUTER, AN INTERNATIONAL LAW OF GUERRILLA WARFARE 20–35 (1984).

as customary international law.[166] Renewed interest in aerial warfare has resulted in the development of the 2009 *Manual on International Law Applicable to Air and Missile Warfare*.[167] By the end of the first decade of the twenty-first century, the United States, as the preeminent world military power, is committed to these legal precautions. This is evidenced by the statements of senior government officials regarding targeting during counterterrorism operations.[168]

Given the pace of technological advances, however, it is clear that the regulation of the cyber domain in either a *jus ad bellum* or *jus in bello* context cannot be allowed to follow the same difficult and tortoise like path to regulation of air warfare as occurred last century. There are signs that this will occur, although it is always necessary to remember that verbal statements to follow fundamental humanitarian law principles regarding aerial warfare were also expressed immediately prior to World War II.[169] There has al-

---

166. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW STUDY 51 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005).

167. PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE (2009), *available at* http://www.ihlresearch.org/amw/manual/.

168. Harold Hongju Koh, Legal Advisor, Department of State, Address at the Annual Meeting of the American Society of International Law (Mar. 25, 2010), *available at* http://www.state.gov/s/l/releases/remarks/139119.htm ("In particular, this Administration has carefully reviewed the rules governing targeting operations to ensure that these operations are conducted consistently with law of war principles. . . ."); Jeh Charles Johnson, General Counsel, Department of Defense, Speech at Yale Law School (Feb. 22, 2012), *available at* http://www.cfr.org/national-security-and-defense/jeh-johnsons-speech-national-security-law-lawyers-lawyering-obama-administration/p27448 ("[T]here is no prohibition under the law of war on the use of technologically advanced weapons systems in armed conflict, so long as they are employed in conformity with the law of war."). Attorney General Eric Holder has also stated, with regard to the use of lethal force:

> Of course, any such use of lethal force by the United States will comply with the four fundamental law of war principles governing the use of force. The principle of necessity requires that the target have definite military value. The principle of distinction requires that only lawful targets – such as combatants, civilians directly participating in hostilities, and military objectives – may be targeted intentionally. Under the principle of proportionality, the anticipated collateral damage must not be excessive in relation to the anticipated military advantage. Finally, the principle of humanity requires us to use weapons that will not inflict unnecessary suffering.

Eric Holder, U.S. Attorney General, Address at Northwestern University School of Law (Mar. 5, 2012), *available at* http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-1203051.html.

169. DOCUMENTS ON THE LAWS OF WAR, *supra* note 162, at 140 (outlining the statement by British Prime Minister Neville Chamberlain on June 21, 1938 on three fundamen-

ready been a commitment by the United States regarding the application of not only the *jus ad bellum*, but also the law of armed conflict to cyber operations conducted during armed conflict.[170] What is not known at this stage is what adherence to broad legal principles means in practical terms during cyber operations or how it will be interpreted in responding to cyber attacks. It is here that the operationalization of international law in the cyber domain by all States will fully demonstrate that commitment. Until the technical, policy and legal communities merge on the cyber highway and "rules of the road" are not only agreed to, but acted upon, it may be the principle of reciprocity that keeps cyber within the lanes as the law catches up to the latest means of warfare that the human mind has developed.[171]

Finally, in assessing the impact of international law on the cyber domain, what cannot be forgotten is that the threshold for armed attack provides, in practical terms, the setting of a threshold for war. As has been noted by David Rodin, wars are hugely complex events, impacted by unpredictable eventualities and which "have a peculiar internal dynamic of their own which often subverts the original objectives and commitments of those who initiate them."[172] Caution will have to be applied in considering the threshold for cyber-based armed attacks given the considerable humanitarian, financial and reputational costs armed conflict inevitably entails.

---

tal principles applicable to aerial warfare: no direct attacks against the civilian population, only target legitimate military objectives and take care to "avoid bombardment of a civilian population in the neighbourhood").

170. *Koh Remarks*, *supra* note 100; *See also* Waxman, *supra* note 44, at 433 n.57 (outlining the testimony of Lieutenant-General Keith Alexander who asserts that returning fire in cyberspace would be lawful "as long as it complied with law of war principles").

171. Eric Schmitt & Thom Shanker, *U.S. Debated Cyberwarfare in Attack Plan on Libya*, NEW YORK TIMES (Oct. 17, 2011), http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html (discussing potential cyber operations to impair Libyan air defenses in March 2011 and explaining that "administration officials and even some military officers balked, fearing that it might set a precedent for other nations, in particular Russia or China, to carry out such offensives of their own").

172. DAVID RODIN, WAR & SELF-DEFENSE 11 (2002).

INTERNATIONAL LAW STUDIES
Est. 1901
U.S. NAVAL WAR COLLEGE

Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations

Jann K. Kleffner and Heather A. Harrison Dinniss

89 INT'L L. STUD. 512 (2013)

Volume 89 2013

Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations

Jann K. Kleffner and Heather A. Harrison Dinniss[*]

I. INTRODUCTION

In recent years it has become an oft-cited truism that the majority of twenty-first century armed conflicts will contain a cyber element. The 2008 conflict between Russia and Georgia was the first publically available indicator of how cyber and conventional force might be used together in an inter-State conflict.[1] Beyond such a relatively clear-cut instance of full-blown international armed conflict, many ongoing situations of crisis, both below and above the level of armed conflict, have attracted a significant and persistent cyber component. Examples include the cyber intifada between Israeli and Palestinian hackers, which has continued since the increase in violence at the outset of the second intifada in 2000; the dispute

* Jann K. Kleffner, Head of the International Law Centre, Associate Professor of International Law, Swedish National Defence College; Heather A. Harrison Dinniss, Postdoctoral Research Fellow, International Law Centre, Swedish National Defence College. The authors gratefully acknowledge the research assistance of Lisen Bergqvist.

1. It should be noted that the attacks against Georgia were not attributed to the Russian Federation, but rather to so-called "patriotic hackers." Analysts did note, however, the high degree of coordination between the actions of the conventional armed forces and the targets of the cyber attacks. For a summary of the reports on the cyber incidents, see ENEKEN TIKK, KADRI KASKA & LIIS VIHUL, INTERNATIONAL CYBER INCIDENTS: LEGAL CONSIDERATIONS (2010).

between India and Pakistan over Kashmir, which has an ongoing and pernicious cyber element involving groups on both sides with varying degrees of alleged State sponsorship; and the Arab Spring, in which many of the States involved used a variety of Internet surveillance, monitoring, censorship and control techniques, and in some cases—notably Tunisia and more recently Syria—hacked the accounts and Internet content of individuals engaged in the revolution.[2]

At the same time, there is a discernible trend on the part of the UN Security Council to authorize various forms of peace operations tasked with an array of functions that are deployed into situations of armed conflicts and other crises. A combination of both trends—the increase of conflict and crisis situations with a cyber component and the deployment of complex peace operations—makes it only natural to assume that peacekeepers will increasingly find themselves on missions in which cyber incidents will occur during, following or even in the absence of, conventional hostilities. Indeed, recent reports have raised the concept of stand-alone cyber peacekeepers. The suggestion that the United Nations should employ specific personnel to deal with the increasing number of cyber incidents taking place between States is indicative of the relevance of cyber operations for the conduct of UN-mandated peace operations.[3] Although the feasibility of cyber-only peacekeeping occurring outside the context of a military operation has been largely dismissed by technical experts,[4] from a purely legal perspective it would certainly be within the purview of the Security Council to determine that cyber operations (whether in a specific situation or as a more general concept) amount to a threat to international peace and security under Article 39 of the UN Charter and to authorize those actions that it considers appropriate.[5]

---

2. BEN WAGNER, DIRECTORATE-GENERAL FOR EXTERNAL POLICIES OF THE EUROPEAN UNION, AFTER THE ARAB SPRING: NEW PATHS FOR HUMAN RIGHTS AND THE INTERNET IN EUROPEAN FOREIGN POLICY 6–13 (2012); Ben Brumfield, *Computer Spyware is Newest Weapon in Syrian Conflict*, CNN (Feb. 17, 2012, 4:41 PM), http://www.cnn.com/2012/02/17/tech/web/computer-virus-syria.

3. Susan Watts, *Call for Cyberwar "Peacekeepers" Force*, BBC NEWS (Jan. 26, 2012, 17:40 GMT), http://news.bbc.co.uk/2/hi/programmes/newsnight/9687338.stm.

4. Ellyne Phneah, *Idea of Cyber Peacekeepers Premature, "Redundant,"* ZDNET NEWS (Feb. 6, 2012, 10:35 GMT), http://www.zdnet.com/idea-of-cyber-peacekeepers-premature-redundant-2062303742/.

5. *See generally* HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 109–13 (2012).

What then are the legal parameters governing peace operations with regard to ongoing cyber threats? Do peacekeepers' responsibilities extend to monitoring cyber threats? When may a peace operation be mandated to conduct cyber operations? How may peacekeepers respond to a cyber attack against them? Are there any legal constraints on a troop-contributing State conducting cyber operations outside the mission area? These are some of the pertinent questions that arise. Answering them from an international law perspective will very much depend on the specifics of the cyber threat, the precise mandate of the peace operation and the operational cyber capabilities of troop-contributing States, among other considerations. We will, therefore, approach the issue in the following manner. First, we will briefly set the general context by defining and describing contemporary peace operations. We will then address the general law applicable to peace operations. Finally, we will discuss the potential types of cyber operations and the legal challenges they pose in more detail.

II. PEACE OPERATIONS DEFINED

For the purposes of this article, peace operations may be defined broadly to include not only traditional peacekeeping operations based on the three core principles of consent, impartiality and the use of force only in self-defense and defense of the mandate, but also peace enforcement operations authorized under Chapter VII of the UN Charter and peace building operations. Chapter VII enforcement differs fundamentally from other peace operations in that it does not require the consent of the target State or entity, and need not be impartial, reactive or restricted to defensive measures.[6] Of particular importance in the cyber context, enforcement measures may also be directed against non-State entities that are deemed to pose a threat to international peace and security. Whether authorized by the Security Council under Chapter VI or VII of the Charter (or under Chapter VIII in the case of regional peacekeeping operations), the legitimacy of the operation flows from the Council's primary responsibility for the maintenance of peace and security, which may be carried out by means of the mandate.[7]

---

6. Terry D. Gill, *Legal Characterisation and Basis for Enforcement Operations and Peace Enforcement Operations under the Charter*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS 85 (Terry D. Gill & Dieter Fleck eds., 2010).

7. *Id.* at 138.

Peace operations have changed dramatically since they began in 1948. In addition to the introduction of enforcement operations in ongoing conflicts, even traditional peacekeeping operations have expanded into complex and multi-dimensional operations. Long established responsibilities of peacekeepers, such as monitoring ceasefires, are now supplemented by tasks which include, *inter alia*, the promotion of a stable environment, maintenance of public order, provision of humanitarian assistance, and protection of civilians from violations of humanitarian and human rights law to the extent possible under the terms of the mandate and the operational capabilities of the particular mission.[8] In future operations, all of these tasks may include a cyber component. The utility of cyber operations in more robust peace operations, including peace enforcement operations, is also apparent. For example, the ability to prepare the battlespace, neutralize networks and uncover and obtain documentary evidence will be useful tools in carrying out particular operations. The type of operation and its constituting mandate are important in determining what cyber operations can be undertaken by a mission.

III. LAW APPLICABLE TO PEACE OPERATIONS

The conceptual underpinning of, and the law applicable to, each type of operation depends on a complex interaction of general international law, human rights law, international humanitarian law and the domestic laws of both the host and troop-contributing States. However, the essential distinction in determining the applicable international legal framework is between those peace operations that fall below the threshold of armed conflict, for which the primary legal framework governing the operation (and any cyber operations which form part of it) is human rights law, and those which occur above that threshold. For operations occurring above the threshold, the law of armed conflict may apply.

A. The Mandate

The principal legal parameter determining the permissibility of actions taken by a peace operation is the mandate established by the Security Council.

8. UNITED NATIONS DEPARTMENT OF PEACEKEEPING OPERATIONS & UNITED NATIONS DEPARTMENT OF FIELD SUPPORT, UNITED NATIONS PEACEKEEPING OPERATIONS: PRINCIPLES AND GUIDELINES 24 (2008), *available at* http://pbpu.unlb.org/pbps/library/capstone_doctrine_eNg.pdf [hereinafter Capstone Doctrine].

It may range from a limited mandate to monitor a peace agreement or ceasefire to a more ambitious one that includes tasks such as protection of civilians, creating a safe and secure environment and training of both civilians and armed forces.[9]

Under Article 41 of the Charter, the Security Council may also mandate non-forceful measures be taken in situations it deems to be a threat to the peace, breach of the peace or act of aggression. Such enforcement measures may include, *inter alia*, partial or total disruption of telecommunications which may well contain a cyber element. Although authorized under Chapter VII and thus not requiring the consent of the host State, such operations fall somewhere between traditional peace operations and the more robust peace enforcement operations that have become common in recent years. Needless to say, not all cyber operations can be treated alike; those which would amount to a use of force would not fall within any mandate provided under Article 41. Whether a cyber operation amounts to a use of force or remains below that threshold raises issues identical to those discussed elsewhere in the present volume.[10]

B. Human Rights

For peace operations falling beneath the threshold of armed conflict, the primary legal paradigm is that of human rights. This includes both peacekeeping operations conducting the more traditional tasks for which the use of force is a last resort in personal and unit self-defense or defense of the mandate, and those authorized under Chapter VII for which the right to use "all necessary means" is authorized, but in which peacekeepers are not involved as combatants in an armed conflict.

Peace operations below the armed conflict threshold may, for instance, involve monitoring the implementation of, and compliance with, a peace agreement, or providing security in a post-conflict environment. In these cases, the international legal framework governing cyber operations is in-

9. For a good illustration of an ambitious mandate, see the United Nations Mission in the Democratic Republic of Congo (MONUC) mandate, containing by some counts no less than forty-nine different tasks for the operation. S.C. Res. 1565, U.N. Doc. S/RES/1565 (Oct. 1, 2004) and resolutions and documents referenced therein [hereinafter MONUC Mandate].

10. *See, e.g.,* William Banks, *The Role of Counterterrorism Law in Shaping* ad Bellum *Norms for Cyber Warfare*, 89 INTERNATIONAL LAW STUDIES 157 (2013); Laurie R. Blank, *International Law and Cyber Threats from Non-State Actors*, *id.* at 406; Noam Lubell, *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, *id.* at 252.

ternational human rights law to the extent that the operation's functions are being exercised in a way that can be equated with the exercise of jurisdiction by a State.[11] States are bound by both international conventions and customary international human rights law. Several court decisions and quasi-judicial determinations have held that States' human rights law obligations do not automatically cease to apply in extraterritorial peace operations, provided that jurisdiction is exercised.[12]

Admittedly, there is no universal consensus on this question. The United States is one of the prominent opponents of the extraterritorial application of human rights law. However, both universal and regional human rights bodies, as well as a significant number of individual States have accepted—or have had to accept—that human rights law does not automatically cease to apply when operating beyond the State's borders. Although the question of when a State exercises extraterritorial jurisdiction has been addressed in numerous cases under the different human rights instruments, it will not be addressed in detail in this article beyond noting that the test may generally be seen as one of effective control over territory, or authority and control over persons.[13]

International organizations such as the United Nations are also bound by customary international law, including human rights law. As with States, if and when an international organization exercises effective control over territory or physical control over one or more persons, the international organization is bound to respect the human rights of those who find themselves within its jurisdiction. In the case of the United Nations, the binding force of international human rights law flows from its international legal personality, and is further strengthened by the UN Charter, the UN Safety Convention,[14] and their internal rules and practice.[15]

---

11. Jann K. Kleffner, *Human Rights and International Humanitarian Law: General Issues*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS, *supra* note 6, at 67.

12. The International Court of Justice, UN Human Rights Committee, European Court of Human Rights and Inter-American Commission on Human Rights have each found that their instruments apply extraterritorially on the basis of jurisdiction.

13. *See generally* MARKO MILANOVIC, EXTRATERRITORIAL APPLICATION OF HUMAN RIGHTS TREATIES: LAW, PRINCIPLES, AND POLICY (2011); Ola Engdahl, *The Future of Human Rights Law in Peace Operations*, *in* LAW AT WAR: THE LAW AS IT WAS AND THE LAW AS IT SHOULD BE 105 (Ola Engdahl & Pål Wrange eds., 2008).

14. Convention on the Safety of United Nations and Associated Personnel, Dec. 9, 1994, 2051 U.N.T.S. 363 [hereinafter UN Safety Convention].

Cyber operations carried out in the context of peace operations below the threshold of an armed conflict are thus governed by such human rights law provisions as the right to privacy, freedom of expression, freedom of association, etc., provided that the person whose rights are at issue finds himself or herself within the jurisdiction of the international organization or troop-contributing State. While the legal basis to conduct cyber operations may stem from the authorization in the Security Council resolution or from self-defence, the actual conduct of such operations is subject to the constraints of human rights law. The UN Human Rights Council has confirmed that "the same rights people have offline must also be protected online."[16] In other words, if jurisdiction is being exercised in a peace operation and it is considered necessary to gather intelligence or conduct operations in the cyber realm—for example, in order to prevent so called "spoilers" from reigniting an armed conflict or to prevent online postings that incite racial hatred—interference with cyber infrastructure or data must be carried out in compliance with the requirements of human rights law.

C. Law of Armed Conflict

When a peace operation involves the conduct of hostilities with a State or organized armed group that crosses the threshold of armed conflict, the law of armed conflict applies. The applicability of that body of law was confirmed in the UN Secretary-General's Bulletin, "[o]bservance by UN Forces of International Humanitarian Law," which sets out the fundamental principles and rules applicable to UN peacekeepers.[17] The bulletin's importance has been reemphasized in "United Nations Peacekeeping Operations: Principles and Guidelines," also referred to as the Capstone Doctrine.[18]

---

15. Kleffner, *supra* note 11, at 67. As examples, Article 1(3) of the UN Charter, which establishes promotion and encouragement of respect for human rights as one of the purposes of the organization, and Decision No. 2005/24 of the Secretary-General's Policy Committee on Human Rights in Integrated Missions, which directs that human rights be fully integrated into peace operations and that all human rights functions be coordinated by one component. Capstone Doctrine, *supra* note 8, at 14, 27.

16. U.N. Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, ¶ 1, U.N. Doc. A/HRC/20/L.13 (2012).

17. U.N. Secretary-General, *Secretary-General's Bulletin: Observance by United Nations Forces of International Humanitarian Law*, U.N. Doc. ST/SGB/1999/13 (Aug. 6, 1999).

18. Capstone Doctrine, *supra* note 8, at 15–16.

While there is little debate over the application of the law to the troops on the ground, a question does remain concerning which entity becomes the party to the armed conflict—the troop-contributing State, the responsible international organization (whether the United Nations, NATO, etc.) or both.[19] Likewise, the determination of whether and for what time the relevant legal actor is to be considered a party to an armed conflict involves complex issues of fact and law that must be determined on a case-by-case basis in light of the factual environment and the operationalization of the mandate for the specific operation within that environment. Some of the factors to be taken into account include, *inter alia*:

- relevant Security Council resolutions;
- specific operational mandates;
- roles and practices actually adopted by the operation during the conflict;
- rules of engagement and operational orders;
- nature of the arms and equipment used by the force;
- interaction between the operation's forces and the parties involved in the conflict, including any use of force between the operation's forces and the parties in an armed conflict, and the nature and frequency of such force; and
- the conduct of the alleged victim(s) and their fellow personnel.[20]

Similarly, whether individual members of a peace operation directly participate in hostilities requires a case-by-case assessment of whether the required threshold of harm, causation and belligerent nexus exists.[21]

Operations in which the hostilities amount to an armed conflict solely between a peace operation and an adversary, with no other parties involved, will be fairly exceptional. It is more likely that a peace operation will be deployed into an ongoing armed conflict or into a volatile situation that then deteriorates into an armed conflict. As it is not a party to the con-

19. For a more detailed examination of the question than is possible in this article, see Ola Engdahl, *Multinational Peace Operations Force Involved in Armed Conflict: Who Are the Parties?*, *in* SEARCHING FOR A "PRINCIPLE OF HUMANITY" IN INTERNATIONAL HUMANITARIAN LAW 233 (Kjetil M. Larsen et al. eds., 2012).

20. *Cf mutatis mutandis* Prosecutor v. Sesay, Kallon and Gbao, Case No. SCSL-04-15-T, Trial Chamber Judgment, ¶ 234 (Special Court for Sierra Leone Mar. 2, 2009).

21. *See generally* NILS MELZER, INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION UNDER INTERNATIONAL HUMANITARIAN LAW (2009).

flict, in these situations the peace operation cannot, without more, conduct military operations that would be subject to the law of armed conflict, nor can it be made the object of attack, whether through cyber means or otherwise. The right to conduct operations governed by the law of armed conflict requires that the peace operation be a party to the armed conflict. If it is not, its members enjoy the protection that international law provides to civilians, as well as the specific protections provided by the UN Safety Convention.

Finally, although controversial and the subject of much scholarly debate, the law of occupation may also apply to peace operations in certain circumstances, whether *de jure* or by analogy.[22] It is sufficient for the purposes of this article to note that territory is only considered occupied when it is *actually* placed under the authority of the occupying force and the law extends only to the territory where that authority has been established and can be exercised.[23] While cyber operations may be used in exercising an occupying power's authority, they would not be sufficient on their own to establish an occupation.[24] Thus, the use of cyber operations to project the execution of a peace operation's mandate into areas outside its effective physical control, for example, by monitoring communications, would not extend the application of the law of occupation to those areas.

We now turn to a more detailed analysis of the general legal framework applicable to different types of cyber operations and the different contexts in which such cyber operations may occur. These scenarios are: first, deployment of a peace operation into a situation of ongoing cyber operations between third parties; second, the use of force by a peace operation in response to cyber attacks; third, cyber operations conducted by a peace operation to protect civilians under imminent threat of physical violence; and, fourth, the conduct of offensive cyber operations by peace operations. Although these different scenarios may overlap to a certain extent, they raise distinct legal issues; hence, they will be treated separately.

---

22. *See, e.g.*, Tristan Ferraro, *The Applicability of the Law of Occupation to Peace Forces*, *in* INTERNATIONAL HUMANITARIAN LAW, HUMAN RIGHTS AND PEACE OPERATIONS 133 (Gian L. Beruto ed., 2008).

23. Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. IV Respecting the Laws and Customs of War on Land art. 42, Oct. 18, 1907, 36 Stat. 2227 [hereinafter Hague Regulations].

24. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE ch. VI cmt. ¶ 3, at 196 (Michael N. Schmitt ed., 2013).

IV. SITUATIONS WHERE THERE ARE ONGOING CYBER OPERATIONS

When peacekeepers find themselves deployed in a situation in which there are ongoing cyber operations between third parties (State-based or otherwise), the mission's obligations and authority with regard to their response to those acts will be dependent on its mandate. However, some general observations may be made.

Clearly, when a peace operation is specifically tasked with acting in situations where there are ongoing cyber operations, it will be authorized to monitor and conduct cyber operations in response to cyber threats. Given the differing capabilities of troop-contributing States in terms of expertise and equipment, however, it seems likely that any specific requirement will contain caveats in terms of acting within the mission's capabilities and resources.[25]

A more likely—and perhaps more interesting—scenario may occur when a peace operation is tasked by the Security Council with deploying into an ongoing security situation that contains a cyber element, but where the mandate does not expressly refer to cyber operations.[26] For example, two of the traditional tasks of peacekeeping operations have been to promote a safe and secure environment and create the conditions for a lasting political solution to a conflict through the monitoring of a ceasefire and the parties' adherence to their commitments under the agreement. In such a case, the generic mandate may be interpreted broadly enough to include the monitoring of Internet traffic, as well as monitoring activities in physical space; however, the permissible methods used to perform those tasks will differ depending on the robustness of the mandate and the level of the

25. Similar wording is currently used with respect to protection of civilians in other peace operations. See, for example, MONUC, which is authorized "*within its capabilities* and in area where its armed units are deployed . . . to ensure the protection of civilians." S.C. Res. 1592, ¶ 5, U.N.Doc. S/RES/1592 (Mar. 30, 2005) (emphasis added). The initial instructions to the African Union mission in Darfur provided that it was to "[p]rotect civilians whom it encounters under imminent threat and in the immediate vicinity *within resources and capability*." Communiqué, Peace and Security Council (Oct. 20, 2004), *available at* http://www.africa-union.org/news_events/Communiqu%C3%A9s/Communiqu%C3%A9%20_Eng%2020%20oct%202004.pdf (emphasis added).

26. This article will restrict itself to the use of technology for monitoring cyber operations. For a discussion of some of the issues raised by intrusive intelligence gathering in peacekeeping operations, see Dieter Fleck, *Individual and State Responsibility for Intelligence Gathering*, 28 MICHIGAN JOURNAL OF INTERNATIONAL LAW 687 (2007); A. Walter Dorn, *The Cloak and the Blue Beret: Limitations on Intelligence in UN Peacekeeping*, 12 INTERNATIONAL JOURNAL OF INTELLIGENCE AND COUNTERINTELLIGENCE 414 (1999).

threat. For example, although all data traffic coming into and out of the mission's networks can be monitored as a matter of good network security, the permissibility of using particular technologies, such as deep packet inspection (DPI),[27] outside of the mission's own networks depends on whether the applicable law permits those actions.

As noted above, both troop-contributing States and the United Nations must comply with human rights law in peace operations in areas subject to their jurisdiction. In the scenario of conducting DPI, the human rights of privacy and freedom of expression come to the fore. Neither of these rights are absolute. International human rights law permits certain interferences with them for reasons of national security and public order.[28] Such exceptions are subject to proportionality requirements. Thus, the parameters established for the use of DPI technology would need to be carefully thought through to avoid casting too wide a net.[29]

It should also be noted in considering multinational operations that in addition to differing approaches to the extraterritorial application of human rights law, judicial approaches to the use of DPI technologies also vary depending on the domestic jurisdiction. The United States and European Union member States, for example, have adopted different standards. Ongo-

---

27. Deep packet inspection involves looking at the content of the packets of information that make up a data stream, rather than merely the TCP/IP routing information contained in the header of the packet. While there are legitimate uses for deep packet inspection that could be valuable to a UN mission (for example, prioritizing particular kinds of data traffic, e.g., Skype), any use that makes the content of the packet available to someone other than the sender and receiver of the message may risk infringing the right to privacy by arbitrarily interfering with communications. Additionally, European Union (EU) member States may run afoul of the EU framework directive on privacy and electronic communications and the EU data protection directive. Directive 95/46/EC of the European Parliament and of the Council (Oct. 24, 1995), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

28. *Cf.* Article 19(3)(b) of the International Covenant on Civil and Political Rights (ICCPR). International Covenant on Civil and Political Rights, G.A. Res. 2200A (XXI), U.N. Doc. A/6316 (Dec. 16, 1966), 999 U.N.T.S. 171. Although Article 17 on the right to privacy contains no explicit reference to exceptions on grounds of national security and public order, it allows for such exceptions, provided an interference with a person's privacy is neither arbitrary nor unlawful.

29. In the words of the Human Rights Committee, restrictions on the right of freedom of expression "must be 'provided by law' [and they] may only be imposed for one of the purposes set out in subparagraphs (a) and (b) of paragraph 3; and they must be justified as being 'necessary' for . . . one of those purposes." Human Rights Committee, General Comment No. 10: Freedom of Expression (Art. 19), U.N. Doc. HR1/GEN/1/rev.1 (June 29, 1983).

ing court cases are in the process of determining the contours of the right of government entities to engage in such behaviors. While the law remains far from settled at the time of this writing, rules of engagement for peace operations deployed in situations where there are ongoing cyber operations should be drafted in such a manner that the permissible limits on the use of DPI or other Internet surveillance technologies are clear. It makes no difference whether the peace operation is conducted with the consent of the host State or the Security Council has authorized the use of "all necessary means" as the rights' holder is the individual. While a Chapter VII mandate would allow States to claim legal authority for surveillance or interception, it is likely that most complaints regarding this technology would relate to the alleged arbitrariness of the surveillance or interception. Differences in interpretation may then be reflected in the national caveats of the troop-contributing States.

Once the applicable law for a peace operation has become the law of armed conflict, the problem is significantly alleviated. Although human rights law continues to apply during armed conflict,[30] the law of armed conflict permits the employment of those measures necessary for obtaining information about the enemy.[31] In fact, parties to an armed conflict are obliged to do so in order to meet the required precautions in attack. Such specific regulations in the law of armed conflict would prevail over the more generic conflicting rules of human rights law (*lex specialis derogat lege generali).*

V. USE OF FORCE IN RESPONSE TO CYBER ATTACKS

Despite the protections afforded to UN personnel,[32] peace operations have increasingly come under attack from those seeking to derail fragile peace processes or manipulate hostile environments for their own purposes. While there is no public record to date on the use of cyber attacks against UN peace operations specifically, other UN organs and the armed forces

30. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226 (July 8); Legal Consequences of the Construction of Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136 (July 9).

31. Hague Regulations, *supra* note 23, art. 24.

32. Protection of UN peacekeepers may stem from their status as civilians under the law of armed conflict or specific treaty protections provided by the UN Safety Convention, *supra* note 14, and its Optional Protocol. Optional Protocol to the Convention on the Safety of United Nations and Associated Personnel, G.A. Res. 60/42, U.N. Doc. A/RES/60/42 (Jan. 6, 2006).

of troop-contributing States have been the subject of cyber operations.[33] There is no reason to believe peace operations will remain untouched by this phenomenon. How then may a peace operation respond to such attacks?

In the first instance, peace operations may be specifically authorized by the mandate to use force to protect its personnel, facilities, installations and equipment.[34] Even absent such an explicit mandate, it is submitted that peace operations also have the authority to use force in response to cyber operations directed against them as an exercise of self-defense, either by an individual soldier, the unit or in extended self-defense (i.e., defense of the mandate.)

At their inception, UN peace operations operated under the principle of non-use of force except in self-defense. The notion of self-defense has subsequently come to include the authority to use force in response to armed attempts to prevent them from carrying out their mandate.[35] Defense of the mandate is now part of the approved UN guidelines and regulations for peacekeeping operations.[36] The right to use force against armed attempts to interfere with the execution of the mandate is not limited to operations authorized under Chapter VII of the UN Charter. It is equally available in more traditional peacekeeping operations, although these operations must also conform with the "bedrock principles of UN Peacekeep-

33. For example, Operation Shady RAT, which was a five-year espionage operation discovered in 2011. It was conducted by an unnamed State actor and directed against multiple entities (companies, governments and non-governmental organizations), including the United Nations. There have also been other low-level attacks specifically directed against UN agencies by non-State groups and individual actors. *See* Dmitri Alperovitch, *Revealed: Operation Shady RAT*, MCAFEE (2011), http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf; *United Nations Agency "Hacking Attack" Investigated*, BBC NEWS (Nov. 29, 2011, 3:58 PM), http://www.bbc.com/news/technology-15951883.

34. See, e.g., the MONUC mandate, which authorizes MONUC to use all necessary means within its capability and in the areas where its armed units are deployed "to ensure the protection of United Nations personnel, facilities, installations and equipment." MONUC Mandate, *supra* note 9, ¶¶ 4(c), 6.

35. Capstone Doctrine, *supra* note 8, at 34.

36. Hans F.R. Boddens Hosang, *Force Protection, Unit Self-Defence, and Extended Self-Defence*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS, *supra* note 6, at 418.

ing, namely impartiality and the necessity of consent and maintenance of consent of all parties to a conflict."[37]

What emerges from the foregoing as important in an examination of the legal parameters governing the use of force against cyber attacks is that the notion of self-defense in the context of peace operations can take on different meanings. It can mean personal self-defense by an individual soldier, unit self-defense or extended self-defense of the mandate. A distinction between those different forms of self-defense is legally relevant because the quintessential requirements for a lawful invocation of any of these, i.e., necessity and proportionality, will lead to different results as to the permissible degree of the use of force.[38]

When a cyber operation directed against a peace operation is severe enough to amount to armed force—that is, it causes death or injury to persons, or physical damage, including loss of functionality, to property and equipment—UN peacekeeping forces are authorized to use force in self-defense to the extent that such use of force complies with the requirements of necessity and proportionality. In other words, the use of force must be necessary to achieve the objective of defending the force and the amount of force must be proportional, that is, it must not greatly exceed the scale and intensity of the attack against which force is used in self-defense.[39] If a cyber operation interferes with the peace operation in such a manner that peacekeeping forces cannot perform their mission (e.g., the command and control systems of the operation have been compromised by a cyber attack) the UN forces would be entitled to use force in defense of the mandate under the same conditions. The use of force by the peacekeeping forces may be kinetic or cyber in nature.

A separate question is the right of a UN peace enforcement operation authorized under Chapter VII to use force against cyber threats that do not themselves amount to a use of force, but which nevertheless interfere with the ability of the enforcement operation to carry out its tasks. When peace enforcement operations are mandated under Chapter VII to use all neces-

37. TERRY D. GILL ET AL., GENERAL REPORT FOR THE 19TH CONGRESS OF THE INTERNATIONAL SOCIETY FOR MILITARY LAW AND THE LAW OF WAR 20 (2012), *available at* http://ismllw.org/congres/2012_05_01_Quebec_General%20Report_Congress-EN.pdf

38. With regard to personal self–defense, see Hans F.R. Boddens Hosang, *Personal Self-Defence and Its Relationship to Rules of Engagement*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS, *supra* note 6, at 429. With regard to force protection and extended self–defense of the mandate, see Hosang, *supra* note 36.

39. GILL ET AL., *supra* note 37, at 10.

sary means, such operations are authorized to enforce the mandate at all times. Consequently, enforcement authority is not limited to defense against armed interference (reactive), but extends to enforcing any element in the resolution in order to restore or maintain international peace and security (proactive).[40]

Ironically, the usual difficulty in positively attributing the source of cyber threats and distinguishing between those that constitute attacks and those that are mere criminal acts may be less problematic in peace operations. When cyber operations are conducted against a peace operation that interferes with carrying out the mandate, the peace operation may respond in self-defense or defense of the mandate regardless of the origin of the attack. Likewise, if the Security Council mandates a peace operation to maintain law and order, contributing States should use all means reasonably available to them to implement the mandate.[41] Thus, the international force can deal with cyber threats that may destabilize the peace operation.

Recent events in which significant unrest has been created by cyber activities illustrate the relevance of this point. For example, in August 2012, a mass exodus of twenty to thirty thousand migrant workers from Bengaluru to their home States in northeastern India was prompted by the combination of SMS, social media and morphed photos appearing to depict violence against Muslims.[42] While the majority of messages appear to have been sent by bulk SMS text and MMS messages, social media and websites have borne the brunt of the government's response to the crisis. In addition to issuing public statements and imposing a ban on bulk text messages, the Indian government blocked 245 webpages for "hosting provocative and harmful content" and has said it will share evidence with the government of Pakistan to back claims that the messages came from that country.[43] If a peace operation mandated with the maintenance of law and order

40. Capstone Doctrine, *supra* note 8, at 34–35; Hosang, *supra* note 36, at 419.

41. Timothy McCormack & Bruce M. Oswald, *The Maintenance of Law and Order in Military Operations*, *in* THE HANDBOOK OF THE INTERNATIONAL LAW OF MILITARY OPERATIONS, *supra* note 6, at 460.

42. In an indication of the dangerous inaccuracy of such media, early figures placed the number of workers fleeing at three hundred thousand.

43. *India to Share Exodus Messages Proof with Pakistan*, BBC NEWS (Aug. 21, 2012, 00:15 AM), http://www.bbc.co.uk/news/world-asia-india-19328364; *India Blames Pakistan for Exodus of Migrant Workers*, BBC NEWS (Aug. 18, 2012, 6:22 PM), http://www.bbc.co.uk/news/world-asia-india-19309982; *State Govts Providing Enough Security to NE People: Centre*, HINDUSTAN TIMES (Aug. 18, 2012), http://www.hindustantimes.com/India-

were confronted with a similar situation, it stands to reason that it could take similar measures, provided that such measures were necessary and proportional under the circumstances.

VI. CYBER OPERATIONS TO PROTECT CIVILIANS

Following a series of tragic incidents, the Security Council has increasingly granted peace operations the authority to use force to "protect civilians under imminent threat of physical violence."[44] The mandate to protect civilians is typically limited to the extent that such protection is possible and within mission capabilities. Conceptually, the right to use force to protect civilians can be viewed, in part, as an extension of the domestic law concept of the right of individual self-defense, which generally allows for defense of a third party, and, in part, as having a distinct basis in the express provisions of the operation's mandate and its attendant rules of engagement.[45] When endowed with such a mandate, a peace operation is entitled to use force when the lives or safety of civilians come under imminent threat of physical danger from a cyber operation, for example, the opening of floodgates on a dam by cyber means. A more difficult question, however, is the ability of the peace operation to use force against a cyber operation that is not so directly linked to physical danger, because the mandate to protect civilians is regularly limited to circumstances where the threats of physical violence are "imminent."

Unfortunately, what the Security Council means by imminence is not clear. Political leaders, UN departments, the UN force commander and national contingent commanders all have an impact on how this term—and the mandate more generally—is interpreted and operationalized in the field.[46] As the Bangalore panic illustrates, cyber operations are certainly capable of making civilian populations believe they are in imminent physical

---

news/NewDelhi/Exodus-continues-30000-NE-people-left-Bangalore-in-3-days/Article1-915431.aspx.

44. S.C. Res. 1590, ¶ 16(1), U.N. Doc. S/RES/1590 (Mar. 24, 2005). The language used by the Security Council in expressly providing for the protection of civilians has been notably consistent over time. *See generally* VICTORIA HOLT & GLYN TAYLOR, PROTECTING CIVILIANS IN THE CONTEXT OF UN PEACEKEEPING OPERATIONS: SUCCESSES, SETBACKS AND REMAINING CHALLENGES 44–47 (2009).

45. GILL ET AL., *supra* note 37, at 22.

46. VICTORIA K. HOLT & TOBIAS C. BERKMAN, THE IMPOSSIBLE MANDATE? MILITARY PREPAREDNESS, THE RESPONSIBILITY TO PROTECT AND MODERN PEACE OPERATIONS 91 (2006).

danger, and, in certain circumstances, cyber operations are linked with very real physical threats. For example, repressive regimes use cyber operations to locate, track and surveil opposition networks and potential dissidents.[47] Whether the correlation between tracking the civilian subjects of that surveillance and their ultimate death or disappearance is direct enough to argue that the imminence requirement is satisfied will depend very much on the context. When the condition is met, the legal justification required for the destruction of the functionality of the surveillance system or the relevant part of it, whether by kinetic or cyber means, may flow from the explicit mandate to protect civilians, or if an explicit mandate to protect civilians is absent, such a legal justification could arguably flow from an extended concept of the right of self-defense.

Irrespective of the legal justification, the use of force to protect civilians under imminent threat of physical violence is constrained by the principles of necessity and proportionality. Both principles would, as a general rule, militate against the necessity of the use of lethal force in response to cyber operations that are the source of an imminent threat. This is because it will generally be possible to counter a cyber threat by technological measures, such as diverting a distributed denial of service (DDoS) attack stream or blocking a port, rather than using lethal force against the person conducting the attack. Given the non-linear progression of technological development, however, the use of force cannot be ruled out. Moreover, as noted previously, the mandate to protect civilians is typically expressed in terms of "to the extent possible" and "within mission capabilities." To date, peace operations, particularly those conducted under the command and control of the United Nations, have had limited technological capacity for intelligence and information analysis[48] and thus may not possess the technical resources or abilities to prevent cyber operations from affecting the civilian population.

The use of force in self-defense—including in defense of the mandate or defense of civilians—does not necessarily mean the forces are involved

47. For an example from Syria, see WAGNER, *supra* note 2; Peter Apps, *Disinformation Flies in Syria's Growing Cyber War*, REUTERS (Aug. 7, 2012, 2:11 PM), http://www.reuters.com/article/2012/08/07/us-syria-crisis-hacking-idUSBRE8760GI20120807.

48. A. Walter Dorn, *United Nations Peacekeeping Intelligence*, *in* THE OXFORD HANDBOOK OF NATIONAL SECURITY INTELLIGENCE 275, 290–92 (Loch K. Johnson ed., 2010).

in an armed conflict such that the laws of armed conflict apply.[49] It is only when a peace operation becomes so actively engaged with a State or organized armed group that hostilities reach the level of armed conflict that the law of armed conflict will apply.[50] In such a case, the right to respond to cyber operations is not constrained by the limits of self-defense; members of the armed forces and military objectives of the adversary may be lawfully attacked. Likewise, of course, the military personnel and military equipment of the peace operation, including military cyber infrastructure and information systems, become lawful targets.

VII. PEACE OPERATIONS CONDUCTING OFFENSIVE CYBER OPERATIONS

To date there is no public record of cyber operations being used by a UN peace operation. The United States has stated that it used cyber operations successfully in Afghanistan.[51] However, given the dual nature of the U.S. presence in the country and the double-hatted command of the troops involved, it is not possible to determine whether the cyber operations were conducted under the auspices of the UN-mandated, NATO-led International Security Assistance Force or the independent U.S. Operation Enduring Freedom. Cyber attacks to disrupt or disable the Libyan air defense networks prior to strikes by coalition aircraft were also contemplated by the United States in that UN-mandated operation, but the idea was discarded in the early stages of operational planning and conventional strikes were ultimately used to achieve the same results.[52] For a peace operation constrained in its use of armed force and likely to be involved in a subsequent transition to reconstruction and development efforts, the ability to

---

49. Ola Engdahl, *The Status of Peace Operation Personnel under International Humanitarian Law*, 11 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 109, 116 (2008); Christopher Greenwood, *International Humanitarian Law and United Nations Military Operations*, 1 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 3 (1998).

50. See *supra* pp. 518-520 for a discussion of the debate on where the threshold lies.

51. Raphael Satter, *US General Says His Forces Carried Out Cyberattacks on Opponents in Afghanistan*, ASSOCIATED PRESS, Aug. 24, 2012, http://seattletimes.com/html/nationworld/2018983462_apusafghancyberattacks.html ("I was able to get inside his nets, infect his command–and–control, and in fact defend myself against his almost constant incursions to get inside my wire, to affect my operations."). A Pentagon spokesman declined to elaborate on the comments, stating merely that the operations were properly authorized and within the bounds of international law. *Id.*

52. Eric Schmitt & Thom Shanker, *U.S. Weighed Use of Cyberattacks to Weaken Libya*, NEW YORK TIMES, Oct. 18, 2011, at A1.

merely turn off a network rather than destroying it means that cyber operations will prove a useful tool in the toolbox of peace operations.

Cyber operations may also allow the mission to project their mandate into regions beyond its area of deployment, which it could not otherwise reach with current capabilities. In addition to their utility for intelligence and monitoring activities, cyber operations provide the ability to remotely shut down the networks of opposing actors, allowing for a significant advantage to a mission seeking to disrupt the activities of those threatening a peace process.

Furthermore, in many circumstances cyber operations provide a mission with a non-forceful method to influence the actors involved in the process, consistent with the principle that a UN peace operation should only use force as a measure of last resort after other methods of persuasion have been exhausted.[53] This includes enabling the mission to take action against outside interference that may be inflaming an already tense situation. For example, the 2007 cyber incidents that accompanied rioting in Estonia were largely conducted from outside the country.[54] Attack scripts were passed in Russian language forums and posted on Russian-hosted websites. Similarly, websites hosting generic attack scripts for use in the cyber elements associated with Operation Cast Lead in the Gaza Strip in 2008 and 2009 were hosted in multiple jurisdictions by both sides. A site called "Help Israel Win" that sought volunteers for a botnet dubbed "Patriot" was moved multiple times in response to attacks from the opposing side. Opposing hacker teams were located in multiple jurisdictions, and included hackers of Saudi Arabian, Egyptian, Turkish, Algerian and Moroccan origin.[55] Comparable situations of outside interference could easily confront a peace operation.

While the specific legal issues raised depend, among other things, on the nature of the cyber action, the type of mandate, applicable law and the facts on the ground, a number of progressively offensive oriented cyber activity examples may prove illustrative of some of the issues involved.

---

53. Capstone Doctrine, *supra* note 8, at 35.

54. *See* TIKK, KASKA & VIHUL , *supra* note 1, at 23 & nn.76–88.

55. GREYLOGIC, PROJECT GREY GOOSE, PHASE II REPORT: THE EVOLVING STATE OF CYBER WARFARE ch. 2 (2009), *available at* http://fserror.com/pdf/GreyGoose2.pdf.

A. Removal or Blocking of Online Content

Online content—whether extremist websites, highly offensive video footage or social media sites—have the potential to inflame, exacerbate and ignite tensions on the ground in areas where the peace operations are working. In some cases, online content may even be a direct incitement to physical violence. Removal of the content could, therefore, contribute to the promotion of a safe and secure environment in accordance with a peace operation's mandate. If webhosts and Internet Service Providers (ISPs) are unable or unwilling to remove the content, can peace operations proactively remove or block access to such materials? One of the factors will be where the content is posted. Peace operation mandates are generally geographically constrained to a specific territory or area of deployment. Thus, the authorization to act provided by the mandate—whether or not it involves the use of force—will be limited to that territory.[56] The same is true of cross-border cyber operations conducted in an effort to remove potentially inflammatory content from sites outside the mission area.

Blocking the availability of particular online content within the geographical confines of the mission area is a far easier way to accomplish the same effect. The most extreme example of governmental intervention in communications technology for security purposes is perhaps the Egyptian government's actions in completely shutting off access to the Internet for four days during the Arab Spring. Other States have taken a more nuanced approach by blocking specific sites or particular content. While States, such as China, with its "great firewall," and regimes in the Middle East and North Africa that engage in heavy web filtering and censorship have technology in place to make such a task easy, other States also have the capacity to engage in such behaviors.[57] For example, India blocked access to approximately 250 websites in an effort to stop the spread of videos and images that caused the Bangalore panic. The Afghan government pushed Internet providers in that country to bar access to websites hosting an anti-Islamic video in order to head off potentially violent demonstrations.[58]

---

56. The exception will be in situations when a peace operation is acting in unit or personal self-defense, which is an inherent right and not linked to the mandate. *See generally* Hosang, *supra* note 36, at 418–27.

57. *See generally*, WAGNER, *supra* note 2.

58. Alissa J. Rubin, *Afghanistan Tries to Block Video and Head Off Rioting*, NEW YORK TIMES (Sept 13, 2012), http://www.nytimes.com/2012/09/14/world/asia/afghanistan-tries-to-block-video-and-head-off-rioting.html?_r=0.

While it appears reasonable to assume that peace operations can block the availability of particular online content within the geographical confines of the mission area on similar legal grounds as provided for by a mandate to protect civilians or one to provide a safe and secure environment, the human rights implications of doing so, particularly for a peace operation under UN command and control, are significant. In a "Joint Declaration on Freedom of Expression and the Internet," rapporteurs on freedom of expression from the United Nations, Organization of American States and the African Commission on Human and Peoples' Rights and the Organization for Security and Cooperation in Europe's representative on freedom from the media stated, "[c]utting off access to the Internet, or parts of the Internet, for whole populations or segments of the public (shutting down the Internet) can *never* be justified, *including on public order or national security grounds*."[59] Although not legally binding, given the breadth of the organizations represented in the declaration, this statement will carry significant weight when applied to a UN peace operation. The right to freedom of expression is not absolute, however, and while blocking entire sections of the Internet may not be justified, restriction of certain content may be appropriate if authorized by the mandate, proportionate under international standards and necessary to protect a recognized interest. Clearly, when the content amounts to incitement to commit crimes, such as genocide or certain other forms of hate speech, blocking of content would be permissible for the peace operation.

B. Neutralization of Command and Control and Air Defense Networks

The ability of cyber operations to neutralize networks without destroying them may prove to be a valuable tool for peace operations. For example, multiphase operations that involve policing no-fly zones or aerial monitoring of disarmament programs may initially benefit from suppression or neutralization of the air defense networks. However, such networks will be needed once peace is restored and the operation moves on to supporting redevelopment.

---

59. Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe Representative on Freedom of the Media, the Organization of American States Special Rapporteur on Freedom of Expression & the African Commission on Human and Peoples' Rights Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration on Freedom of Expression and the Internet*, ¶ 6(b) (2011) (emphases added).

Whether neutralizing, but not destroying, such a network is legally permissible depends on the categorization of the acts and the mandate of the particular operation. There has been a great deal of debate whether mere neutralization of a network by cyber means would amount to an attack under the laws of armed conflict.[60] Agreement appears to have been reached that destruction of the functionality of objects, to include network components, such that a physical component has to be replaced would amount to an attack.[61] The same analysis may be used in evaluating whether actions by a peace operation constitute a use of force. Therefore, merely turning a network off as a proactive measure would not overstep an authorization limiting the use of force to that necessary in self-defense.[62] Other potential restrictions on taking such an action would be dependent on the mandate for the particular operation and the associated rules of engagement.

Neutralization of computers engaging in cyber operations from outside the area of operations, such as against international "spoilers" that take part in DDoS attacks similar to those directed against Estonia, face the same geographical constraints outlined in the previous section with regard to removal of content. At the same time, peace operation mandates in Security Council resolutions almost always call on member States to provide assistance to peace operations. In some cases they require States to ensure that their nationals, individuals and firms within their territory or subject to their jurisdiction refrain from particular behaviors.[63] As a result, peace operations are able to call on the member State in which the perpetrators are located or of which they are nationals to assist in preventing "spoiler" activities and punishing those who engage in such activities. Simultaneously, the peace operation could block and/or redirect the DDoS traffic emanating from particular Internet Protocol addresses using ISPs or webhosts located in the geographical area of the peace operation.

---

60. *See, e.g.*, HARRISON DINNISS, *supra* note 5, at 196–202.

61. TALLINN MANUAL, *supra* note 24, at 105–110.

62. Clearly, however, if the network had actually been used against aircraft involved in the peace operation or indicated hostile intent, e.g., by acquiring a radar lock on an operation aircraft, any use of force against the system would be authorized as self-defense.

63. *See*, *e.g.*, S.C. Res. 1973, ¶¶ 9, 19, 21, U.N. Doc S/RES/1973 (Mar. 17, 2011), concerning general assistance by UN member States to the UN-authorized Libya operation and the specific tasks States were to take in support of the freeze on Libyan assets.

C. Destruction of Surveillance or Command and Control Capabilities

When more destructive offensive cyber measures are envisaged, such as those causing physical damage to equipment of the opposing party in non-self-defense circumstances, authorization must derive from the mandate. As noted above, physical destruction by cyber means is a use of armed force and must, therefore, be authorized by the Security Council. Since traditional peacekeeping missions are authorized only to use force in self-defense as defined above, offensive cyber operations are not permitted. Peace enforcement operations endowed with a Chapter VII authorization to use "all necessary means," may, on the other hand, use force to enforce the mandate. Thus, offensive cyber operations causing damage, destruction or personal injury are authorized in any situation that kinetic force would be permissible, provided they are necessary to fulfill mission objectives. Likewise, when members of the peace operation find themselves actively engaged in hostilities under the laws of armed conflict, destructive offensive cyber operations may be used against military objectives in accordance with that body of law.[64]

VIII. CONCLUSION

The foregoing analysis confirms that a detailed answer of the legal parameters governing peace operations that confront or conduct cyber operations cannot be provided in the abstract. The mandates and capabilities of peace operations and the contexts in which they are deployed are too varied and complex. Nonetheless, one can draw some general conclusions.

First, it seems certain that cyber operations directed against or conducted by peace operations can be expected to increase. Second, it would appear equally reasonable to assume that the majority of instances in which peace operations are involved in cyber operations—either as actors engaging in such activity or as the object of cyber operations of other actors—will take place when the peace operation is not a party to an armed conflict; hence, it will not be operating under the law of armed conflict. To the extent this is true, international human rights law will remain at the fore as the main international legal framework governing cyber operations.

Whether operating under a law of armed conflict regime or a human rights regime, peace operations will always be able to conduct cyber opera-

64. *See, e.g.*, Banks, *supra* note 10; Blank, *supra* note 10; Lubell, *supra* note 10.

tions of some type. Indeed, the importance of cyber capabilities is likely to increase in light of their operational utility and efficiency. Exactly what type of cyber operation will be legally permissible, and how intrusive, disruptive and offensive it may be, will however, ultimately depend on the specific mandate.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Cyber Warfare: Implications for Non-international Armed Conflicts

Robin Geiss

89 INT'L L. STUD. 627(2013)

Volume 89 2013

Cyber Warfare: Implications for Non-international Armed Conflicts

Robin Geiss[*]

I. INTRODUCTION

Cyberspace is considered by many to be a new warfighting domain.[1] Legal discussions concerning warfare in this domain have primarily focused on the level of the *ius ad bellum*[2] and international armed conflicts.[3] With the exception of action on cybercrime, especially the 2001 European Convention on Cybercrime and tentative attempts to design a similar instrument

* Professor at the Faculty of Law, University of Potsdam, Potsdam, Germany.

1. U.S. DEPARTMENT OF DEFENSE, QUADRENNIAL DEFENSE REVIEW REPORT 37 (2010) [hereinafter QUADRENNIAL DEFENSE REVIEW REPORT].

2. Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE JOURNAL OF INTERNATIONAL LAW 421 (2011); HEATHER H. DINNISS, CYBER WARFARE AND THE LAWS OF WAR 37 (2012); Duncan B. Hollis, *An e-SOS for Cyberspace*, 52 HARVARD INTERNATIONAL LAW JOURNAL 373 (2011); Marco Roscini, *World Wide Warfare:* Jus ad Bellum *and the Use of Cyber Force*, 14 MAX PLANCK UNITED NATIONS YEARBOOK 85 (2010).

3. Michael N. Schmitt, *Wired Warfare: Computer Network Attack and* Jus in Bello, 84 INTERNATIONAL REVIEW OF THE RED CROSS 365 (2002); Sean Watts, *Combatant Status and Computer Network Attack*, 50 VIRGINIA JOURNAL OF INTERNATIONAL LAW 392 (2010).

on the global level,[4] the focus of contemporary discussions has primarily been on inter-State issues and State-sponsored cyber operations. Conversely, the relevance of cyber warfare in non-international armed conflicts and the corresponding legal challenges arising under the laws of armed conflict have only rarely been addressed.[5]

One reason is certainly the notion that non-international armed conflict today encompasses such a wide range of rather different scenarios,[6] ranging from low-intensity armed conflicts between organized armed groups in failed-State scenarios like Somalia[7] to traditional types of civil war like the ongoing armed conflict in Syria to "internationalized" scenarios like the armed conflict in Afghanistan,[8] that the relevance of cyber warfare in a particular conflict varies widely. Quite clearly, in many non-international armed conflict scenarios sophisticated cyber weaponry is without significant military relevance. Nevertheless, when parties to a non-international armed conflict rely on cyber infrastructure and cyber operations to further their strategic aims, cyber operations will also become increasingly relevant. The Syrian government, for example, has repeatedly shut off the Internet

4. Marco Gercke, *Ten Years [after the] Convention on Cybercrime: Achievements and Failures of the Council of Europe's Instrument in the Fight against Internet-Related Crimes*, 12 COMPUTER LAW REVIEW INTERNATIONAL 142 (2011); UNITED NATIONS OFFICE ON DRUGS AND CRIME, THE GLOBALIZATION OF CRIME 218 (2010) [hereinafter GLOBALIZATION OF CRIME]; Susan W. Brenner, *Cybercrime, Cyberterrorism and Cyberwarfare*, 77 REVUE INTERNATIONALE DE DROIT PENALE 454 (2006).

5. Rather the focus has been on potential terrorist attacks by non-State actors. *See, e.g.*, Kelly A. Gable, *Cyber-Apocalypse Now: Securing the Internet Against Cyberterrorism and Using Universal Jurisdiction as a Deterrent,* 43 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 59 (2010).

6. Sylvain Vité, *Typology of Armed Conflicts in International Humanitarian Law: Legal Concepts and Actual Situations*, 91 INTERNATIONAL REVIEW OF THE RED CROSS 75 (2009); Marko Milanovic & Vidan Hadzi-Vidanovic, *A Taxonomy of Armed Conflict*, *in* RESEARCH HANDBOOK ON INTERNATIONAL CONFLICT AND SECURITY LAW (Nigel D. White & Christian Henderson eds., forthcoming 2013**)**; SANDESH SIVAKUMARAN, THE LAW OF NON-INTERNATIONAL ARMED CONFLICT (2012).

7. Robin Geiss, *Armed Violence in Fragile States: Low-intensity Conflicts, Spillover Conflicts, and Sporadic Law Enforcement Operations by Third Parties,* 91 INTERNATIONAL REVIEW OF THE RED CROSS 134 (2009).

8. Robin Geiss & Michael Siegrist, *Has the Armed Conflict in Afghanistan Affected the Rules on the Conduct of Hostilities?*, 93 INTERNATIONAL REVIEW OF THE RED CROSS 11, 13–14 (2011).

to block opposition groups' channels of communication,[9] U.S. drones have reportedly been hacked by Iraqi insurgents,[10] and websites used by Al-Qaida have repeatedly been hacked and manipulated by the U.S. Department of State,[11] although it remains, of course, controversial as to whether the latter activities have occurred in the context of a non-international armed conflict.[12] Moreover, as Stuxnet and other malware tools proliferate, it may be only a question of time before non-State actors will be able to carry out more sophisticated cyber operations. Against this backdrop, this article seeks to discuss particular legal issues arising under the laws of armed conflict with regard to the use of military cyber operations in non-international armed conflicts. The analysis proceeds in three steps and will analyze three general questions.

The first question that arises when considering the issue of cyber warfare in non-international armed conflicts is whether cyber operations in and of themselves, without accompanying kinetic military operations, could ever trigger a non-international armed conflict.[13] In view of the relatively high threshold required for a non-international armed conflict, it appears this could happen only in the most exceptional cases. Nevertheless, States

---

9. *See Syria Internet Services Shut Down as Protesters Fill Streets*, WASHINGTON POST (June 3, 2011, 9:58 AM), http://www.washingtonpost.com/blogs/blogpost/post/syria-internet-services-shut-down-as-protesters-fill-streets/2011/06/03/AGtLwxHH_blog.html.

10. *See US Drones Hacked by Iraqi Insurgents*, GUARDIAN (Dec. 17, 2009, 3:02 PM), http://www.guardian.co.uk/world/2009/dec/17/skygrabber-american-drones-hacked.

11. *See* David P. Fidler, *Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law*, AMERICAN SOCIETY OF INTERNATIONAL LAW INSIGHTS (June 20, 2012), http://www.asil.org/pdfs/insights/insight120620.pdf; Hillary Clinton, U.S. Secretary of State, Remarks at the Special Operations Command Gala Dinner (May 23, 2012), http://www.state.gov/secretary/rm/2012/05/190805.htm; Benjamin Wittes, *State Department Hackers?*, LAWFARE (May 24, 2012, 7:08 AM), http://www.lawfareblog.com/2012/05/state-department-hackers/. *See, e.g.*, *Hillary Clinton Boasts of US Cyberwar against Al-Qaeda*, TELEGRAPH (May 24, 2012, 6:00 AM), http://www.telegraph.co.uk/news/worldnews/al-qaeda/9286546/Hillary-Clinton-boasts-of-US-cyberwar-against-al-Qaeda.html; *Hacking Terrorist Websites Commonplace*, THE INVESTIGATIVE PROJECT ON TERRORISM (June 3, 2011, 1:32 PM), http://www.investigativeproject.org/2937/hacking-terrorist-websitescommonplace; Adam Rawnsley, *Stop the Presses! Spooks Hacked al-Qaida Online Mag*, WIRED (June 1, 2011, 1:56 PM), http://www.wired.com/dangerroom/2011/06/stop-the-presses-spooks-hacked-al-qaida-online-mag/.

12. *See* Claus Kress, *Some Reflections on the International Legal Framework Governing Transnational Armed Conflicts,* 15 JOURNAL OF CONFLICT AND SECURITY LAW 245, 261, 266 (2010).

13. *See* Schmitt, *supra* note 3, at 368.

are concerned that sophisticated non-State actors could launch severe attacks against modern States in which civil society, the economy and financial markets are increasingly reliant on a functioning, unimpeded cyber infrastructure.[14] Indeed, while States have become much more aware of their cyber vulnerabilities—the Clinton administration issued a presidential directive on critical infrastructure protection as early as in 1998[15]—some technical experts maintain that significant vulnerabilities remain and that ultimately only disconnecting critical systems from networks could bring about a satisfactory degree of protection.[16]

At this time, it is difficult to determine the significance of the cyber threat presented by non-State actors. Non-State actors committing cyber crime[17] and economic cyber espionage[18] do pose serious threats, but to date there have been no public reports of significant and highly devastating cyber attacks launched by non-State actors against a State. There is widespread agreement among experts that cyber operations like Stuxnet and Flame, in view of their complexity and sophistication, could only have been carried out by a State, by a coalition of States or at least with significant State support.[19] Therefore, on the yet-to-be-proven assumption that non-State actors could wage highly destructive cyber operations upon States,

---

14. *See* Gable, *supra* note 5, at 73; *Intelligence Community Annual Threat Assessment: Hearing Before the S. Select Comm. on Intelligence*, 111th Cong. 39 (2009) (statement of Dennis C. Blair, Director of National Intelligence), *available at* http://intelligence.senate.gov/090212/blair.pdf ("Terrorist groups, including al-Qai'da, HAMAS, and Hizballah, have expressed the desire to use cyber means to target the United States.").

15. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, May 22, 1998, *available at* http://www.fas.org/irp/offdocs/pdd/ pdd-63.htm.

16. SANDRO GAYCKEN, CYBERWAR—DAS WETTRÜSTEN HAT LÄNGST BEGONNEN 235–36 (2012).

17. COUNCIL OF EUROPE, CONVENTION ON CYBERCRIME: EXPLANATORY REPORT, *available at* http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm (last visited Sept. 13, 2012); Roderic Broadhurst, *Developments in the Global Law Enforcement of Cyber-crime*, 29 POLICING: AN INTERNATIONAL JOURNAL OF POLICE STRATEGIES AND MANAGEMENT 415 (2006), *available* at http://www.emeraldinsight.com/journals.htm?articleid=1571786& show=abstract.

18. *See, e.g.*, OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE, FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE (2011), *available at* http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

19. *See Cyberattacks on Iran—Stuxnet and Flame*, NEW YORK TIMES (Aug 9, 2012), http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html.

this article will assess whether and under what circumstances such operations in and of themselves could trigger the application of the laws of armed conflict.

The second question that arises when considering the issue of cyber warfare in non-international armed conflicts relates to the geographic scope of application of the laws of armed conflict. Cyberspace by definition transgresses all national boundaries. It defies any classic notion of a delimited battlefield and enables parties to an armed conflict to launch cyber operations from just about anywhere in the world, to target any network that is connected to cyberspace and to use components of the global cyber infrastructure (servers, cables, etc.) for military purposes. Therefore, it appears that the controversial debate over the geographic scope of application of the laws of armed conflict pertaining to non-international armed conflicts is of particular relevance in the cyber domain.

Finally, the third question relates to the use of cyber operations in the course of an already ongoing non-international armed conflict in which conventional kinetic military means and methods of warfare are being employed. It is now widely accepted that there is no legal vacuum in cyberspace[20] and that "[e]xisting principles of international law apply online, just as they do offline."[21] The critical question, however, is what particular legal challenges arise under the rules governing the conduct of hostilities in non-international armed conflicts when means and methods of cyber warfare are employed?[22] In order to answer these questions, it first needs to be determined what kind of cyber operations are likely to be employed in non-international armed conflicts before, in a second step, discussing the particular challenges arising under the laws of armed conflict.

---

20. *No Legal Vacuum in Cyber Space*, Interview with Cordula Droege, International Committee of the Red Cross (Aug. 16, 2011), http://www.icrc.org/eng/resources/ documents/interview/2011/cyber-warfare-interview -2011-08-16.htm.

21. Joe Biden, Vice President of the United States, Remarks at the London Conference on Cyberspace (Nov. 1, 2011), http://www.whitehouse.gov/photos-and-video/video/2011/11/01/vice-president-biden-delivers-remarks-london-conference-cyberspace#transcript .

22. Robin Geiss, *The Legal Regulation of Cyber-attacks in Times of Armed Conflict*, *in* BRUGES COLLOQUIUM, TECHNOLOGICAL CHALLENGES FOR THE HUMANITARIAN LEGAL FRAMEWORK 47 (College of Europe & International Committee of the Red Cross eds., 2011), *available at* http://www.coleurope.eu/sites/default/files/uploads/page/collegium_41_0.pdf.

II. CAN CYBER OPERATIONS BY THEMSELVES TRIGGER A NON-INTERNATIONAL ARMED CONFLICT?

In order to determine whether cyber operations alone could bring into existence a non-international armed conflict, it needs to be assessed whether, and, if so, under what circumstances, the requisite threshold of violence and the degree of organization required with regard to the armed group involved is reached.

A. The Intensity Requirement

As is well known, in the *Tadić* judgment the International Criminal Tribunal for the former Yugoslavia (ICTY) affirmed that a non-international armed conflict exists only when there is "protracted armed violence."[23] This formula has consistently been applied not only in the case law of the ICTY, but also by other tribunals, namely, the International Criminal Court (ICC), the International Court of Justice, the International Criminal Tribunal for Rwanda and the Special Court for Sierra Leone.[24] What is more, according to Article 1(2) of Additional Protocol II and Article 8(2)(d) and (f) of the ICC Statute, as well as customary international law, situations of internal disturbances and tensions, riots or sporadic acts of violence and other acts of a similar nature do not meet the required threshold of violence.[25] In order to facilitate the assessment of whether there is "protracted armed violence," the ICTY considers various indicative criteria such as the gravity of attacks and their recurrence,[26] the number of victims,[27] the temporal and

23. Prosecutor v. Tadić, Case No. IT-94-1-l, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the former Yugoslavia Oct. 2, 1995) [hereinafter *Prosecutor v. Tadić*]; Vité, *supra* note 6.

24. *See* ANTHONY CULLEN, THE CONCEPT OF NON-INTERNATIONAL ARMED CONFLICT IN INTERNATIONAL HUMANITARIAN LAW 121 nn.19–25 (2010).

25. *See* Prosecutor v. Jean-Pierre Bemba Gombo, Case No. ICC-01/05-01/08, Decision on the Confirmation of Charges, ¶ 225 (Pre-Trial Chamber II June 15, 2009; Anthony Cullen, *The Definition of Non-International Armed Conflict in the Rome Statute of the International Criminal Court: An Analysis of the Threshold Contained in Article 8(2)(f)*, 12 JOURNAL OF CONFLICT AND SECURITY LAW 419, 429 (2007).

26. Prosecutor v. Slobodan Milošević, Case No. IT-02-54-T, Trial Chamber Decision on Motion for Judgment of Acquittal (Rule 98bis Decision), ¶ 28 (Int'l. Crim. Trib. for the former Yugoslavia June 16, 2004) [hereinafter *Prosecutor v. Milošević*].

territorial expansion of violence[28] and the collective character of hostilities.[29]

Against this backdrop, it appears that no cyber attack has ever risen to the requisite threshold of violence. In terms of intensity, not even the Stuxnet operation, the only publicly known cyber operation (with the possible exception of the mysterious Siberian pipeline incident of 1982)[30] that has directly caused physical destruction in the "real world," approached the threshold of violence commonly required for a non-international armed conflict.[31] What is more, even though ICTY trial chambers have interpreted the criterion of "protracted armed violence" as referring more to the intensity of the armed violence than to its duration,[32] it follows from the explicit caveat contained in Article 1(2) of Additional Protocol II,[33] which is also considered reflective of customary international law with regard to Common Article 3 of the four 1949 Geneva Conventions,[34] that singular and merely sporadic cyber incidents, including those that directly cause physical damage or injury, would not amount to a non-international armed conflict. Clearly, mere network intrusions, cyber exploitation operations, data theft and data manipulation, as well as random denial-of-service attacks carried out by a non-State actor, while they would fall into the realm of domestic

---

27. *Id.*

28. *Id.*, ¶ 29.

29. Prosecutor v. Limaj, Case No. IT-03-66-T, Judgment (Trial Chamber), ¶¶ 94–134, 170 (Int'l Crim. Trib. for the former Yugoslavia Nov. 30, 2005); Prosecutor v. Haradinaj, Case No. IT-04-84-T, Judgment (Trial Chamber), ¶ 49 (Int'l Crim. Trib. for the former Yugoslavia Apr. 3, 2008); *see* EVE LA HAYE, WAR CRIMES IN INTERNAL ARMED CONFLICTS 9–13 (2010).

30. William Safire, *The Farewell Dossier*, NEW YORK TIMES, Feb. 2, 2004, at A21, *available at* http://www.nytimes.com/2004/02/02/opinion/the-farewell-dossier.html.

31. In fact, in the case of Stuxnet as far as can be seen no State—including Iran—has publicly qualified the incident as either an "armed attack" or an "armed conflict." *See, e.g.*, Gary Brown & Keira Poellet, *The Customary International Law of Cyberspace*, 6 STRATEGIC STUDIES QUARTERLY 132 (2012).

32. *Prosecutor v. Haradinaj, supra* note 29, ¶ 49.

33. "This Protocol shall not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts." Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts art. 1(2), June 8, 1977, 1125 U.N.T.S. 609. *See also* COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, ¶ 4471 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987).

34. CULLEN, *supra* note 24, at 108; *see* SIVAKUMARAN, *supra* note 6, at 105.

criminal law[35] and could arguably amount to "attacks" in the sense of Article 49 of Additional Protocol I if carried out in the context of an already ongoing armed conflict,[36] would not suffice to trigger a non-international armed conflict in view of the intensity threshold required for this particular armed conflict category. Therefore, while there may be some possibility that cyber operations by non-State actors in exceptional cases may reach the critical threshold of violence, it does not appear to be a likely scenario.

B. The Required Degree of Organization

In addition, for a non-international armed conflict to come into existence, a second criterion also needs to be fulfilled. As the ICTY has held, an armed conflict can exist only between parties that are sufficiently organized to confront each other with military means.[37] While it has rightly been pointed out that the required degree of organization should not be exaggerated,[38] in order to be sufficiently "organized" a non-State armed group must be under an established command structure and must have the capacity to sustain military operations.[39] In the *Lubanga* decision, the ICC Pre-Trial Chamber held that "the involvement of armed groups with *some degree of organization* and the ability to plan and carry out sustained military operations would allow for the conflict to be characterized as an armed conflict not of an international character."[40]

The explicit reference to "some degree of organization" is indicative of the uncertainty as to the exact degree of organization required. In part, this is due to the fact that, notwithstanding universal agreement about the requirement's existence, it has never fully been clarified nor is there full agreement about the criterion's precise function and purpose and why an armed group must be organized in the first place.[41] Is it because only an organized armed group can be expected to sustain military operations on a level that meets the required intensity threshold? Or must an armed group

35. *See* GLOBALIZATION OF CRIME, *supra* note 4, at 203.

36. *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE rule 30 (Michael N. Schmitt ed., 2013).

37. *See Prosecutor v. Tadić, supra* note 23, ¶ 70.

38. Claus Kress, *The 1999 Crisis in East Timor and the Threshold of the Law on War Crimes,* 13 CRIMINAL LAW FORUM 409, 416 (2002).

39. *See Prosecutor v. Limaj*, *supra* note 29, ¶ 129.

40. Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Decision on the Confirmation of Charges, ¶ 233 (Pre-Trial Chamber I Jan. 29, 2007) (emphasis added).

41. TALLINN MANUAL, *supra* note 36, cmt. to rule 23, ¶ 15.

be organized because only then can it be expected to ensure that its members abide by the laws of armed conflict?[42] The 2008 Report of the International Law Association's Use of Force Committee seems to support the former reading. It suggests that "[t]he criteria of organization and intensity are clearly related and should be considered together when assessing whether a particular situation amounts to an armed conflict. It seems that the higher the level of organization the less degree of intensity may be required and vice versa."[43] This assessment, of course, also leaves open the questions of the required minimum degree, if any, of organization and whether high intensity operations of only loosely organized or even unorganized actors could suffice.

Of course, it is beyond any doubt that armed groups like the Taliban and the Revolutionary Armed Forces of Colombia (the FARC) meet the requisite degree of organization. If distinct armed groups with a similarly high degree of organization launched cyber operations that reach the required intensity threshold, a non-international armed conflict would be triggered. At the same time, however, it is equally clear that cyber operations and computer network attacks by private individuals would not suffice. Such actions may invoke domestic criminal law, but not the laws of armed conflict. Even when a number of individual actors are acting collectively—for example in a spontaneous denial-of-service attack that finds more and more online followers or by sharing and spreading malware tools—they do not qualify as an organized armed group. Collective action—or even organized action—without more is neither sufficient nor decisive.

What matters is the existence of a distinct armed group and that that particular group has a visible and verifiable organizational structure.[44] Thus, the ICTY, when assessing the organizational structure of the Kosovo Liberation Army, referred, *inter alia*, to factors such as the existence of military headquarters,[45] the adoption of internal regulations,[46] the nomination of a

42. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 33, ¶ 4470 (regarding Article 1(1) of Additional Protocol II); *see also* TALLINN MANUAL, *supra* note 36, cmt. to rule 23, ¶ 14 n.202.

43. Committee on the Use of Force, International Law Association, Initial Report on the Meaning of Armed Conflict in International Law 22 (2008) [hereinafter Meaning of Armed Conflict]; *see* Vité, *supra* note 6, at 76.

44. *See Prosecutor v. Limaj*, *supra* note 29, ¶¶ 89–90.

45. *Id.*, ¶ 90; *Prosecutor v. Milošević, supra* note 26, ¶¶ 23–24.

46. *See Prosecutor v. Limaj*, *supra* note 29, ¶¶ 98, 113–17.

spokesperson,[47] and the issuance of orders, political statements and communiqués,[48] as well as the establishment of military police and disciplinary rules.[49] Similarly, in the *Callixte Mbarushimana* decision the ICC Pre-Trial Chamber referred, *inter alia*, to the Democratic Forces for the Liberation of Rwanda's (FDLR's) hierarchical structure and high level of internal organization, the existence of a political and a military wing, and the FDLR's constitutive instruments, which included "a statute, a '*règlement d'ordre intérieur*' and a disciplinary code which provided the organization's internal disciplinary system."[50]

More recently, there have been discussions about whether so-called "virtual groups," i.e., groups that are organized exclusively on-line and consist of people dispersed over various locations, could be qualified as organized armed groups.[51] Setting aside the controversial question of international humanitarian law's geographic scope of application, it appears that merely virtual groupings that have no physical infrastructure, such as headquarters, physical meeting points, etc., would be too elusive to qualify as a reference point for the determination of the existence of a non-international armed conflict. What is more, due to the notorious human-machine gap in cyberspace, that is, the problem of identifying the natural person behind a given computer, it would be almost impossible to determine membership in a virtual group with any degree of certainty. Of course, over time using extensive forensic investigations and the means and methods of law enforcement such a determination may be possible, but within the narrow time frame that is typically available in a conduct of hostilities context it seems unrealistic.

Moreover, it appears that the different criteria referred to in the *Limaj* judgment and the *Callixte Mbarushimana* decision—albeit only non-exclusive and indicative—inherently presuppose a certain degree of effective control exercised through a chain of command of the group concerned. And, although it may be possible to issue orders online irrespective of geographic distance between the members of a virtual group, the means to enforce such orders are significantly limited when the connection between the

47. *Id.*, ¶¶ 99, 102.

48. *Id.*, ¶ 101.

49. *Id.*, ¶ 113.

50. Prosecutor v. Mbarushimana, Case No. ICC-01/04-01/10, Decision on the Confirmation of Charges, ¶ 104 (Pre-Trial Chamber I Dec. 16, 2011).

51. TALLINN MANUAL, *supra* note 36, cmt. to rule 23, ¶ 13 (a virtual organization is one "in which all activities that bear on the criterion [organization] occur on-line").

members of the group is only virtual. Therefore, the idea that a decentralized virtual group of persons in different locations—possibly dispersed all over the globe—could constitute an organized armed group in the sense of the laws of armed conflict should be dismissed. While it is undeniable that genuine and important security interests of States may be affected by the activities of such virtual groups, the laws of armed conflict hardly serve as a panacea to solve cyber security issues on a global level.

III. THE GEOGRAPHIC SCOPE OF APPLICATION OF THE LAWS OF ARMED CONFLICT IN THE CYBER CONTEXT

Cyberspace is a decentralized, global medium that transgresses national boundaries and defies any notion of a delimited battlefield.[52] The fact that cyber attacks can be launched from anywhere in the world with launch-to-impact times being reduced to milliseconds[53] certainly adds to the controversy regarding the geographic scope of application of the laws of armed conflict in non-international armed conflicts.[54] Is a Taliban fighter who launches a cyber attack from Islamabad, Pakistan against International Security Assistance Force (ISAF) member States still subject to the laws of armed conflict and thereby a legitimate military target? Is the individual hacker who operates out of Buenos Aires and launches cyber attacks against ISAF's communication infrastructure in Afghanistan thereby rendered a legitimate military target? Or is he only a criminal hacker subject to domestic law enforcement in Argentina?

It is not the purpose of this article to revisit or engage in a detailed review of this familiar debate that has been laid out extensively elsewhere.[55] In any case, as far as military operations against persons are concerned, the legal questions that arise in the cyber context are no different from those that arise with regard to the highly controversial practice of extraterritorial targeted killings. Suffice it to say, a number of authors agree that the notion of non-international armed conflict as set forth in Common Article 3 is not confined to single-State scenarios, but also comprises a certain cross-

52. *See* DINNISS, *supra* note 2.

53. Robin Geiss, *War and Law in Cyberspace: The Conduct of Hostilities in and via Cyberspace,* 104 AMERICAN SOCIETY OF INTERNATIONAL LAW PROCEEDINGS 371 (2011).

54. *See* SIVAKUMARAN, *supra* note 6, at 250–52 nn.102–20.

55. *See, e.g.*, Derek Jinks, *September 11 and the Laws of War,* 28 YALE JOURNAL OF INTERNATIONAL LAW 1 (2003); MARCO SASSÒLI, TRANSNATIONAL ARMED GROUPS AND INTERNATIONAL HUMANITARIAN LAW (2006); Kress, *supra* note 12.

border dimension.[56] Opinions vary, however, on whether this cross-border dimension is regionally confined to so-called "spill-over scenarios"[57] or whether it may warrant a wider, arguably even global, application of the laws of armed conflict.[58] The wording of Common Article 3 is sufficiently broad to accommodate a cross-border dimension, and in the case of spill-over conflicts, where national boundaries are randomly and frequently crossed, pragmatic reasons and the geographic proximity to the original armed conflict may support such an interpretation.[59] Nevertheless, the various definitions of non-international armed conflict as they are laid out in treaty law, whether in Common Article 3, Article 1(1) of Additional Protocol II or Article 8(2)(f) of the ICC Statute, and the ICTY's ruling in *Tadić*, all contain a territorial link of some sort.[60] Against this background, and in light of the fact that the laws of non-international armed conflicts constitute a reaction to extreme levels of military violence (hence the high threshold requirements laid out above),[61] multi-State application that pays no heed to the geographical proximity to ongoing hostilities cannot, in the view of the present author, be sustained.[62]

Cyber warfare, by virtue of the technological nature of cyberspace, adds an additional aspect to the debate. Every cyber operation carried out via the Internet (except where malware is implanted directly into the target system as was the case with Stuxnet) typically uses cyber infrastructure components in different locations around the globe. Therefore, in the case of cyber warfare, the issue of geographic scope of application of the laws of

---

56. Milanovic & Hadzi-Vidanovic, *supra* note 6; NOAM LUBELL, EXTRATERRITORIAL USE OF FORCE AGAINST NON-STATE ACTORS 101–4 (2010); Dapo Akande, *Classification of Armed Conflicts: Relevant Legal Concepts, in* INTERNATIONAL LAW AND THE CLASSIFICATION OF CONFLICTS 32, 46–47 (Elizabeth Wilmshurst ed., 2012).

57. Jelena Pejic, *The Protective Scope of Common Article 3: More Than Meets the Eye*, 93 INTERNATIONAL REVIEW OF THE RED CROSS 189 (2011).

58. GEOFFREY S. CORN, VICTOR M. HANSEN, DICK JACKSON, ERIC TALBOT JENSEN & JAMES A. SCHOETTLER JR., THE WAR ON TERROR AND THE LAWS OF WAR: A MILITARY PERSPECTIVE 11 (2009)

59. Pejic*, supra* note 59, at 193.

60. The ICC Chamber in the *Bemba Gombo* decision therefore concluded that an armed conflict not of an international character "takes place within the confines of a State territory." *Prosecutor v. Bemba Gombo*, *supra* note 25, ¶ 231.

61. *See supra* notes 23–36 and accompanying text.

62. *See* YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 56 (2d ed. 2010) ("from the vantage point of international law . . . a non-international armed conflict cannot possibly assume global dimensions").

armed conflict is as relevant to the targeting of objects involved in cyber operations as it currently is with regard to persons.

Certainly, in an international armed conflict involving highly sophisticated military forces and large-scale cyber operations, a vast percentage of the worldwide civilian and dual-use cyber infrastructure will be used for military purposes, potentially posing a considerable challenge to the law of neutrality. But the trans-boundary nature of cyberspace and the dual-use character of the global cyber infrastructure may also play out in non-international armed conflicts. The following, admittedly rather simplistic, example may help to illustrate the point. Taliban fighters install a botnet—a worldwide network of remote-controlled civilian computers[63]—in order to generate computer power to launch a cyber operation against the communication infrastructure of States supporting the Afghan government in its fight against the Taliban. All the civilian systems unknowingly involved in the botnet are used to make an effective contribution—however individually minimal—to military action. Collectively they are the infrastructure used to carry out a cyber operation and thus would arguably qualify as legitimate military objects in accordance with the definition contained in Article 52 of Additional Protocol I, which is generally accepted as being reflective of customary international law in both international and non-international armed conflicts.[64]

Of course, it could be argued that even when certain components of the global cyber infrastructure are used for military purposes, this does not automatically render them a military objective because in the interconnected and largely resilient domain of cyberspace destroying or temporarily disrupting a server that is used for military purposes by non-State actors would not offer a definite military advantage since the cyber operation can be easily switched to other servers. Under these circumstances, destroying or disrupting individual components would not diminish the attacker's capacity to execute further cyber operations. After all, Article 52(2) and the corresponding customary law rule contain a two-pronged test. In order to qualify as a legitimate military objective, an object must not only be used to make an effective contribution to military action, but its destruction must

63. An example is the Mariposa botnet, which reportedly involved an estimated 13 million systems in over 190 countries. *See* Joseph Menn, *Investigators Shut Down Mariposa Hacking Network*, FINANCIAL TIMES, Mar. 4, 2010, World News, at 7.

64. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW rule 8, at 29 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005).

also offer a definite military advantage in the circumstances ruling at the time.[65]

It appears doubtful, however, that Article 52(2)'s military advantage requirement will function as an effective constraint. Although the law clearly requires a two-pronged test when qualifying military objectives, the interplay of these two tests has remained ambiguous. In practice, the emphasis is usually placed only on the first. As the commentary in the *Air and Missile Warfare Manual* confirms, "[i]n practical terms, compliance with the first criterion [the requirement of nature, location, purpose or use] will generally result in the advantage required of the second."[66]

It must be noted that only if there is an assumption of a multi-State or global application of the laws of non-international armed conflicts can the use of the worldwide cyber infrastructure for military purposes by non-State actors potentially render its components military objectives. Article 52 and the customary law definition of legitimate military objectives are only of relevance when the laws of armed conflict apply in the first place. In traditional non-international armed conflicts, the use of State or civilian property by organized armed groups undisputedly rendered these objects legitimate military objectives. The problem is that cyberspace has enabled States and non-State actors to use State and civilian cyber infrastructure components located in countries around the world.

Yet it is far from clear that this justifies an automatic extension of the scope of application of the laws of armed conflict. In essence, this would allow non-State actors to turn components of the worldwide cyber infrastructure into legitimate military objectives basically by virtue of a few mouse clicks. Within milliseconds during a single cyber attack various data packages may randomly travel via different channels all over the world, thereby arguably using all of these channels to make an effective contribution to military action. A global application of the laws of armed conflict that encompasses any militarily useful cyber activity wherever it may occur would rapidly lead to a large-scale militarization of cyberspace and could obviously have far-reaching destabilizing effects on relations between States.

---

65. Robin Geiss & Henning Lahmann, *Cyber-Warfare: Applying the Principle of Distinction in an Interconnected Space,* 45 ISRAEL LAW REVIEW 1, 7 (2012).

66. PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, COMMENTARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE 49 (2010).

Absent a specific legal regime of neutrality relating to non-international armed conflicts,[67] *ius ad bellum* rules constrain military operations against cyber infrastructure in third States even if components of this infrastructure qualify as legitimate military objectives. However, if military operations are regarded as permissible in cases where States are unable due to lack of expertise or technology to stop physical cyber infrastructure located on their territory from being used to carry out cyber operations against other States,[68] *ius ad bellum* rules may not impose a significant constraint in the cyber context. Currently, even States with the most advanced cyber technology are often unable to detect and immediately end malicious cyber activity that occurs on, or originates from, their territory, let alone attribute such operations to individual persons.

IV. CYBER OPERATIONS AS A METHOD OF WARFARE IN NON-INTERNATIONAL ARMED CONFLICTS IN WHICH THERE ARE TRADITIONAL KINETIC MILITARY OPERATIONS

While there is little doubt that military cyber operations will become increasingly relevant in future non-international armed conflicts, currently the focus of military strategists is principally on inter-State scenarios and international armed conflicts.[69] This is reflected in contemporary legal literature on cyber warfare, which has largely focused on the laws of armed conflict as they apply in international armed conflicts.[70] In future inter-State armed conflicts that involve high-tech belligerents with sophisticated cyber capabilities and corresponding vulnerabilities, gaining information dominance—i.e., control over cyberspace and outer space—will become as important a strategic goal as obtaining control over territory, airspace or the

67. The law of neutrality applies only during international armed conflicts. *See* TALLINN MANUAL, *supra* note 36, ch. VII, ¶ 1.

68. *Id.*, cmt. to rule 13, ¶ 22. The "unable and unwilling" standard, however, remains controversial. *See* TOM RUYS, ARMED ATTACK AND ARTICLE 51 OF THE UN CHARTER—EVOLUTIONS IN CUSTOMARY LAW AND PRACTICE (2010).

69. *See, e.g.*, Secretary of Defense, Sustaining U.S. Global Leadership: Priorities for 21st Century Defense (2012), *available at* http://www.defense.gov/news/Defense_Strategic _Guidance.pdf.

70. *See, e.g.*, Schmitt, *supra* note 3; Watts, *supra* note 3; Eric Talbot Jensen, *Cyber Warfare and Precautions Against the Effects of Attacks,* 88 TEXAS LAW REVIEW 1533, 1542 (2010); KNUT DÖRMANN, APPLICABILITY OF THE ADDITIONAL PROTOCOLS TO COMPUTER NETWORK ATTACKS (2004), *available at* http://www.icrc.org/eng/assets/files/other/ applicability ofihltocna.pdf; Geiss, *supra* note 55.

sea has been in traditional conflicts.[71] As the U.S. Quadrennial Defense Review Report emphasizes, "in the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace."[72]

Military cyber operations in future inter-State armed conflicts will aim to degrade the enemy's capacity to use cyberspace for military operations, to manipulate the enemy's data and the functioning of its cyber-connected systems, and to block the enemy's ability to communicate via cyberspace. It is well known that sophisticated military forces of major States are already preparing for potential future cyber battlefields by preimplanting concealed codes and software tools in various strategically relevant "places," as well as by manipulating hardware components along the supply chain.[73] This type of cyber warfare will not only use cyberspace as a medium to deliver attacks against "real world" military targets (e.g., launching a cyber attack against an electrical power plant that is used for military purposes), but will also include large-scale kinetic military operations against strategically relevant cyber infrastructure components, including software and hardware, all over the globe.

Cyber warfare in non-international armed conflicts will likely feature only some of these aspects of cyber war between States. While fears have been expressed that non-State actors could use cyber operations to enhance their military capabilities and to attack critical infrastructure of States, it is not clear that non-State actors currently have that capacity. Yet, the cyber vulnerabilities of organized armed groups against which cyber attacks could be conducted also remain limited. Even though some of the States currently involved in the non-international armed conflict in Afghanistan are heavily reliant on cyber capabilities for their military operations in Afghanistan,[74] the Taliban do not appear to have the technological ability to attack these capabilities or even interfere with them to any significant

71. QUADRENNIAL DEFENSE REVIEW REPORT, *supra* note 1, at 37.

72. *Id.*

73. *See* BRYAN KREKEL, PATTON ADAMS & GEORGE BAKOS, NORTHRUP GRUMMAN CORPORATION, OCCUPYING THE INFORMATION HIGH GROUND: CHINESE CAPABILITIES FOR COMPUTER NETWORK OPERATIONS AND CYBER ESPIONAGE 11–12 (2012) ("By providing counterfeit hardware that already contains the Trojanized access built into the firmware or software, a foreign intelligence service or similarly sophisticated attacker has a greater chance of successfully penetrating these downstream supply chains." *Id.* at 11).

74. Wayne W. Grigsby Jr., Garrett Howard, Tony McNeill & Gregg Buehler, *CEMA: A Key Success in Unified Land Operations,* 62 ARMY MAGAZINE 44 (2012).

degree. Conversely, the reliance of the Taliban on cyber assets or systems connected to cyberspace to carry out military operations or attacks—apart perhaps from the use of mobile telephones for military communications and the remote detonation of improvised explosive devices (IEDs)[75]—also appears to be limited.

Of course, the situation may be different if third States become involved in a non-international armed conflict. Thus, in the currently hypothetical scenario of an intervention by third States in the ongoing non-international armed conflict in Syria, it is certainly conceivable that cyber operations would be used to disable Syrian air defense systems. Needless to say, however, that intervention of external States would lead to an international armed conflict between the intervening States and Syria, in addition to the already ongoing non-international armed conflict.

In traditional non-international armed conflicts, i.e., those in which other States do not intervene, it seems that cyber warfare in the strict sense of the actual conduct of hostilities is today of only rather limited relevance. Rather, cyberspace is used for vastly different purposes, namely, using social media and media reporting for public information purposes and political mobilization. Even though it is likely that with the rapidly growing worldwide dependence on cyberspace, further technological evolution and the proliferation of malware tools, the relevance of cyberspace will increase in non-international armed conflicts, the legal questions that arise in relation to the conduct of hostilities in such conflicts are generally similar to those arising in international armed conflicts.

Thus, when cyberspace is used as a medium to deliver attacks against "real world" targets, as opposed to "virtual targets," typically no particular legal challenges will arise. Whether a legitimate military objective, such as a military communications center, is attacked via cyberspace or by an airstrike, the same legal principles apply.[76] Clearly, any attacker planning to carry out such an attack would be bound, *inter alia*, by the principle of pro-

75. Mobile telephones are often a vital military instrument for organized armed groups in various parts of the world; they are used to detonate bombs and to coordinate military movements and operations.

76. *See* Geiss & Lahmann, *supra* note 67. The precautions in attack norm is codified in Article 57 of Additional Protocol I for international armed conflict, whereas the rule of proportionality is codified in Articles 51 and 57.

portionality and would be required to take precautions in accordance with customary international law.[77]

Moreover, as in international armed conflicts, it may be questionable whether a particular operation qualifies as an "attack" in the legal sense of Article 49 of Additional Protocol I, which, by virtue of customary international law, also applies to non-international armed conflicts.[78] It appears, however, that various aspects of this debate have now been settled by the definition in the *Tallinn Manual*, according to which "[a] cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects," which by and large appears to reflect widespread consensus.[79]

Controversy persists only with regard to the question of whether damage and destruction also encompass the temporary loss of functionality in cases where no direct physical damage results.[80] For example, computerized systems may be manipulated via cyberspace in order to shut down connected systems. Thus, the distribution of electrical energy could be stopped by virtue of data manipulation in the control systems of power grids and power plants with no direct physical destruction. Such operations may be strategically appealing, particularly in non-international armed conflicts where States will aim to deprive their non-State enemies of strategic assets such as electrical power, while leaving the underlying infrastructure intact. It is clear that not every military operation that causes inconvenience for the civilian population—for example, a roadblock—automatically qualifies as an attack in the legal sense.[81] It is also clear that collective punishments and the terrorization of the civilian population are strictly prohibited under all circumstances.[82] Nevertheless, there is nothing in the laws of armed conflict that would bar an interpretation that qualifies an operation leading to the loss of functionality—irrespective of how this loss is caused and whether this involved physical destruction—as an attack. In fact, the overall object and purpose of the rules governing the conduct of hostilities—"to ensure respect for and protection of the civilian population and civilian

77. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 64, rules 15–21, at 51–67.

78. Schmitt, *supra* note 3, at 368–75; TALLINN MANUAL, *supra* note 36, cmt. to rule 30, ¶¶ 1–19.

79. TALLINN MANUAL, *supra* note 36, rule 30.

80. *Id.*, cmt. to rule 30, ¶ 10.

81. Geiss, *supra* note 55.

82. 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, *supra* note 64, rule 103, at 374 and rule 8, at 29.

objects"[83]—would generally seem to militate in favor of a broader, rather than a more limited, understanding of the notion of attack, given that only attacks in the legal sense are subject to the principle of distinction and proportionality.

V. CONCLUSION

At present, many of the issues pertaining to non-international armed conflicts and cyber warfare remain the subject of some speculation. In particular, the military cyber capabilities that non-State actors currently have, or may develop, is unclear. Though it appears highly unlikely that cyber attacks by a non-State actor could alone trigger a non-international armed conflict, specific cyber attacks in the course of an ongoing conflict in which traditional kinetic forms of attack are occurring are certainly conceivable. As far as legal issues pertaining to the actual conduct of hostilities are concerned, the legal questions raised are generally the same as those that are currently being discussed with regard to international armed conflicts. There is widespread agreement that cyberspace is not a legal vacuum and that international law, including the laws of armed conflict, applies in cyberspace. But in view of the dual-use nature of the entire cyber infrastructure and the fact that the artificial domain of cyberspace transgresses State boundaries, it seems that an unrestrained application of the laws of armed conflict, especially those relating to non-international armed conflicts, could lead to an unwarranted large-scale militarization of cyberspace. Quite clearly, therefore, the laws pertaining to non-international armed conflicts should be applied cautiously in the cyber domain and, in view of the unique and still insufficiently understood technical features of cyberspace and the possibilities for its military use, the precise parameters of their application need to be worked out more concretely than they have been to date.

83. *Id.*, rule 1, at 3; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts art. 48, June 8, 1977, 1125 U.N.T.S. 3.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

The Law of Armed Conflict's "Wicked" Problem: *Levée en Masse* in Cyber Warfare

David Wallace
Shane R. Reeves

89 INT'L L. STUD. 646 (2013)

Volume 89 2013

The Law of Armed Conflict's "Wicked" Problem: *Levée en Masse* in Cyber Warfare

David Wallace
Shane R. Reeves[*]

The defense of the nation, an insurrection of the people must be initiated. . . . There is absolutely no time for delay.

Walther Rathenau, "A Dark Day" (1918)[1]

Cyberspace is the new frontier, full of possibilities to advance security and prosperity in the 21st century. And yet, with these possibilities, also come new perils and new dangers. The Internet is open. It's highly accessible, as it should be. But that also presents a new terrain for warfare. It is a battlefield of the future where adversaries can seek to do harm to our country, to our economy, and to our citizens. But the even greater danger —the greater danger facing us in cyberspace goes beyond crime and it goes beyond harassment. A cyber attack perpetrated by nation states [or] violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation.

U.S. Secretary of Defense Leon E. Panetta[2]

---

* David Wallace is a Colonel in the United States Army and a Professor and the Deputy Head, Department of Law at the United States Military Academy, West Point, New York. Shane Reeves is a Major in the United States Army and an Assistant Professor at the United States Military Academy, West Point.

1. Michael Geyer, *People's War: The German Debate About a Levée en Masse in October 1918*, *in* THE PEOPLE IN ARMS: MILITARY MYTH AND NATIONAL MOBILIZATION SINCE THE FRENCH REVOLUTION 124 (Daniel Moran & Arthur Waldron eds., 2003).

2. Leon E. Panetta, Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City (Oct. 11, 2012).

I. INTRODUCTION

Attempting to categorize and label a contemporary armed conflict is a complicated task. Not restricted to "hot battlefields,"[3] and an amalgamation of asymmetric and conventional tactics, modern wars escape traditional conflict classifications.[4] International or non-international armed conflict and irregular or conventional war are no longer workable distinctions as conflict participants now engage "along a broad spectrum of operations and lethality."[5] These aptly titled "hybrid armed conflicts"[6] create an unpredictable operational environment[7] that is exacerbated by ever-increasing civilian participation in hostilities[8] and the emergence of new technologies.[9] Prognostica-

3. "Hot battlefields" is a term used to reference geographically contained conflicts. For example, Afghanistan, or, until recently, Iraq would be construed as a hot battlefield. *See*, *e.g.*, Ashley S. Deeks, *Pakistan's Sovereignty and the Killing of Osama Bin Laden*, AMERICAN SOCIETY OF INTERNATIONAL LAW INSIGHTS, http://www.asil.org/insights110505.cfm (last visited Feb. 9, 2012)("the most controversial aspect . . . is the U.S. argument that this conflict can and does extend beyond the "hot battlefield" of Afghanistan to wherever members of al Qaeda are found").

4. U.S. DEPARTMENT OF DEFENSE, QUADRENNIAL DEFENSE REVIEW REPORT 8 (2010) [hereinafter QDR] (discussing the difficulty in categorizing contemporary conflicts).

5. *See* Robert Gates, U.S. Secretary of Defense, Remarks at Maxwell Air Force Base, Alabama (Apr. 15, 2009), http://www.defense.gov/transcripts/transcript.aspx? transcriptid=4403 (noting "black and white distinction[s] between irregular war and conventional war is an outdated model"); *see also* QDR, *supra* note 4, at 8.

6. *See* QDR, *supra* note 4, at 8 (stating "[t]he term 'hybrid' has recently been used to capture the seemingly increased complexity of war, the multiplicity of actors involved, and the blurring between traditional categories of conflict."); *see also* Shane R. Reeves & Robert E. Barnsby, *The New Griffin of International Law: Hybrid Armed Conflicts*, HARVARD INTERNATIONAL REVIEW, Winter 2013, at 16–18, *available at* http://hir.harvard.edu/mobile-might/the-new-griffin-of-war (discussing the international legal challenges presented by hybrid warfare).

7. *See* U.S. Department of the Army, TRADOC Pam. 525-3-1, The United States Army Operating Concept 2016–28, ¶ 2-2(a) (2010) [hereinafter CAPSTONE CONCEPT].

8. *See* INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 7 (Nils Melzer ed., 2009) [hereinafter ICRC Interpretive Guidance], *available at* http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf (stating "there is little reason to believe that the current trend towards increased civilian participation in hostilities will weaken over time").

9. *See* QDR, *supra* note 4, at 80.

tors believe this trend towards ambiguity in armed conflict is becoming the norm rather than the exception.[10] Perhaps no domain in modern warfare more starkly validates this prediction than cyberspace.[11]

Applying the law of armed conflict, as currently constructed, in this environment is "highly problematic"[12] as legal obligations are almost impossible to discern.[13] Recognizing this problem, the NATO Cooperative Cyber Defence Centre of Excellence recently enlisted an international group of experts, led by Professor Michael Schmitt of the Naval War College, to draft the *Tallinn Manual on the International Law Applicable to Cyber Warfare* "to help government's deal with the international legal implications of cyber operations."[14] In hopes of providing clarity for those governments, this recently published work attempts to explain how the existing law of armed conflict

10. *See* CAPSTONE CONCEPT *supra* note 7, ¶ 2-2(a); QDR, *supra* note 4, at iii.

11. CAPSTONE CONCEPT *supra* note 7, ¶ 5-7(a) (stating "[a] critical enabler for virtually all elements of national and military power, cyberspace has become an increasingly contested domain."). The overarching importance of cyberspace in modern warfare cannot be overstated. *See e.g.*, RICHARD A. CLARKE & ROBERT K. KNAKE, CYBER WAR: THE NEXT THREAT TO NATIONAL SECURITY AND WHAT TO DO ABOUT IT 69 (2010); Stephen W. Korns & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, PARAMETERS, Winter 2008–09, at 60 (discussing the desperate actions of the Georgian government after it found itself unable to communicate through the Internet during the 2008 Georgian-Russian conflict); William C. Ashmore, *Impact of Alleged Russian Cyber Attacks,* 11 BALTIC SECURITY & DEFENSE REVIEW 4 (2009) (discussing the adverse effects of the 2007 cyber attack on Estonia); David E. Sanger, David Barboza & Nicole Perlroth, *Chinese Army Unit Is Seen as Tied to Hacking Against U.S.*, NEW YORK TIMES, Feb. 18, 2013, at A1 (describing a series of aggressive cyber attacks carried out by Unit 61398, a Chinese military unit, against various U.S. government agencies and corporations and the potential responses).

12. Korns & Kastenberg *supra* note 11, at 71.

13. Stephen Daggett, Congressional Research Service, R41250, Quadrennial Defense Review 2010: Overview and Implications for National Security Planning 2 (2010); *see also* Nils Melzer, *Keeping the Balance Between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 831, 833 (2010)(discussing the difficulties in contemporary armed conflicts due to the "blurring of the traditional distinctions and categories upon which the normative edifice of IHL has been built").

14. *See, e.g.*, *Manual Examines How International Law Applies to Cyberspace,* IT WORLD, (Sept. 3, 2012), http://www.itworld.com/legal/293042/manual-examines-how-international-law-applies-cyberwarfare (noting that The Cooperative Cyber Defense Center of Excellence, which "assists NATO with technical and legal issues associated with cyber warfare related issues," created the *Tallinn Manual* to address a variety of cyber legal issues).

generally regulates cyber warfare.[15] However, when specific provisions of the law of armed conflict are applied in cyber warfare, it is apparent that generalities do not address the truly "wicked" nature of the problem.[16] One particular example—trying to reconcile the concept of *levée en masse* with the "cyber conflicts between nations and ad hoc assemblages"—illustrates how ill-suited, and often impractical, the existing law of armed conflict can be when applied in the cyber context.[17]

To support this proposition, this article will begin with a brief discussion on the history of a *levée en masse*. An explanation of how the law of armed conflict defines and characterizes the individual battlefield status associated with *levée en masse* will follow. The article will then explore the unique aspects of hostilities in cyberspace and delve into the impracticality of applying the concept of *levée en masse* in the context of cyber warfare. It will conclude with specific recommendations in terms of the reconceptualising of a *levée en masse* in cyber warfare and a hope that, by focusing on this nuanced provision of the law of armed conflict, a broader discussion will ensue.

II. PEOPLE IN ARMS—HISTORY AND BACKGROUND ON THE LEVÉE EN MASSE

A distinct type of resistance movement in warfare has been the collective uprising limited to the actual period of the invasion of a territory—a *levée en masse*.[18] Having acquired something of a mythical status in the history of war,[19] the underlying concept of a *levée en masse* is simply that during the initial invasion, the civilian population of unoccupied territory can spontaneously take up arms against the invading army in order to forestall an occupa-

15. The *Tallinn Manual* examines the "international law governing cyber warfare" and encompasses both *jus ad bellum* and the *jus in bello*. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 4 (Michael Schmitt ed., 2013).

16. "Wicked problems" are generally defined as extraordinarily complex and tricky issues that evade traditional solutions. *See generally* Horst W.J. Rittel & Melvin M. Webber, *Dilemmas in a General Theory of Planning,* 4 POLICY SCIENCES 155 (1973). Instead, novel and creative ideas are required to develop a workable answer as a definitive solution may never be possible. *Id.* at 162–63.

17. Korns & Kastenberg *supra* note 11, at 70.

18. KARMA NABULSI, TRADITIONS OF WAR: OCCUPATION, RESISTANCE, AND THE LAW 52 (2004).

19. *See* Karma Nabulsi*,* Levée en Masse, CRIMES OF WAR (Mar. 11, 2013), http://www.crimesofwar.org/a-z-guide/levee-en-masse/ (stating "[t]he *levée en masse*, or mass uprising, has acquired something of a mythical status in the history of war.").

tion.[20] Underpinning the revolutionary mobilization of a l*evée en masse* is patriotic zeal coupled with the initiative of the citizen-soldier under emergency circumstances.[21] The *levée en masse* institutionalizes total war in the context of the defense of a nation,[22] with all members of the community having a role until the enemy had been repelled or defeated.[23] As both territorial occupation and spontaneity are defining characteristics, a *levée en masse* is a key legal classification of participants typically during an early and brief period of an armed conflict.

The law of armed conflict recognizes that a *levée en masse* occurs when inhabitants of a non-occupied territory, without time to form into a regular armed unit, spontaneously take up arms to resist an invading force.[24] *Levée en masse* participants are considered lawful combatants and are entitled to prisoner-of-war status if they carry arms openly and respect the laws and customs of warfare.[25] Endowing *levée en masse* participants with lawful combatant status recognizes—and reinforces—the belief that "[t]he first duty of a citizen is to defend his country, and provided he does so loyally he should not be treated as a marauder or criminal."[26] The Lieber Code, the Brussels Declaration, the Hague Regulations, and the Third Geneva Convention all expressly encapsulate in positive legal provisions the special status given to *levée en masse* participants.[27]

---

20. YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 42 (1st ed. 2004).

21. Dierk Walter, *Reluctant Reformers, Observant Disciples: The Prussian Military Reforms, 1807–1814*, *in* WAR IN AN AGE OF REVOLUTION 1775–1815, at 87, 87 (Roger Chickering & Stig Forster eds., 2010).

22. Scott Lytle, *Robespierre, Danton, and the* Levée en Masse, 30 JOURNAL OF MODERN HISTORY 325, 325 (1958).

23. Alan Forrest, *The French Revolution and the First* Levée en Masse*, in* THE PEOPLE IN ARMS: MILITARY MYTHS AND NATIONAL MOBILIZATION SINCE THE FRENCH REVOLUTION 14 (Daniel Moran & Arthur Waldron eds., 2003).

24. Convention Relative to the Treatment of Prisoners of War art. 4(A)(6), Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter GC III]; GARY SOLIS, THE LAW OF ARMED CONFLICT: INTERNATIONAL HUMANITARIAN LAW IN WAR 200–201(2010)(citing Prosecutor v. Delalić, IT-96-21-T, Judgment, ¶ 268 (Int'l Crim. Trib. for the former Yugoslavia Nov 16, 1998)).

25. GC III, *supra* note 24, art. 4A(6).

26. MORRIS GREENSPAN, THE MODERN LAW OF LAND WARFARE 62 (1959).

27. JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, 2 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW: PRACTICE 2545–50, §§49–80 (2005) [hereinafter PRACTICE] (discussing the historical acceptance of the concept of *levée en masse*).

The concept of a *levée en masse* is deeply rooted in history with its origins firmly planted in the French Revolution.[28] The French Revolution marked a dramatic shift from dynastic warfare between kings to mass participation of the populace as citizens took up arms to defend their national soil.[29] Based on a principle of the nation in arms, the armies of the French Revolution represented a significant departure from centuries of tradition regarding military organization for warfare.[30] On August 23, 1793, the National Convention under the leadership of its Committee of Public Safety, in one of the most celebrated decrees of the French Revolution,[31] issued the following statement:

> From this moment until that in which every enemy has been driven from the territory of the Republic, every Frenchman is permanently requisitioned for service with the armies. The young men shall fight; married men will manufacture weapons and transport stores; women shall make tents and nurse in the hospitals; children shall turn old linen into lint; the old men shall report to the public square to raise the courage of the warriors and preach the unity of the Republic and hatred against the kings.[32]

Accordingly, military units were formed on a territorial basis. In September 1793, recruiting under the *levée en masse* decree provided over 450,000 men for the French armies.[33] On October 15 of that year, the concept of *levée en masse* was validated at the Battle of Wattignies as a viable form of warfare when the French citizen-army successfully beat back invading regular military units from Austria.[34]

The French, though formalizing the term and concept, are by no means alone in using a *levée en masse*; history is replete with other examples. The

---

28. Emily Crawford, Levée en Masse–*A Nineteenth Century Concept in a Twenty-First Century World* 3 (Sydney Law School, Legal Studies Research Paper No. 11/31, May 2001), *available at* http://ssrn.com/abstract=1851947 (noting that the concept originated with the French Revolution of 1789).

29. *See* Audrey Kurth Cronin, *Cyber-Mobilization: The New Levée en Masse*, PARAMETERS, Summer 2006, at 77, 77–78.

30. GUNTHER E. ROTHENBERG, THE ART OF WARFARE IN THE AGE OF NAPOLEON 95 (1980).

31. *Id.* at 100.

32. Lytle, *supra* note 22, at 325.

33. ROTHENBERG, *supra* note 30, at 100–110.

34. SOLIS, *supra* note 24, at 200.

Prussian *Erhebung*, or uprising, fueled the War of Liberation in 1813[35] as Prussian citizens, displaying patriotic feelings and a popular willingness to accept sacrifice, flocked to the colors to throw off the French yoke.[36] In 1864, during the United States Civil War, 257 cadets from the Virginia Military Institute formed a *levée en masse* to fight the approaching Union forces at the Battle of New Market.[37] In the closing months of World War I, a significant debate arose among both the German military and national public about the possibility of "going French" and waging a people's war—a *volkskrieg*—against the allies.[38] For a variety of political, military and practical reasons, the Germans ultimately decided not to use a *levée en masse* to defend the "fatherland."[39]

During World War II, in response to the German invasion of the Soviet Union (Operation Barbarossa), the Soviet's placed "[n]early all inhabitants of the country from teenagers to the elderly . . . on call for either labor or military duty, and the distinctions between military and civilian life were once again erased."[40] Professor Gary Solis, in his award winning book on the law of armed conflict, provides a compelling account of a *levée en masse* on Wake Island. He states, in part, as follows:

> On December 24, 1941, two weeks after Pearl Harbor, U.S.-held Wake Island fell to invading Japanese forces. More than eleven hundred American civilian construction workers were among the island's population. 'More than sixty civilians are known to have taken part in the ground fighting and their valor—if not their combat skills—equaled that of the servicemen.' One hundred twenty-four Americans died before Wake Island was forced to surrender. Seventy-five of the dead were civilians who manned shore batteries and heavy machine guns, held defensive positions and, when Japanese infantry landed, fought in counterattacks.[41]

In the aftermath of the Balkans War, the International Criminal Tribunal for the former Yugoslavia examined the question of whether a *levée en masse*

---

35. Daniel Moran, *Arms and the Concert: The Nations in Arms and the Dilemmas of German Liberalism*, in THE PEOPLE IN ARMS: MILITARY MYTHS AND NATIONAL MOBILIZATION SINCE THE FRENCH REVOLUTION 52 (Daniel Moran & Arthur Waldron eds., 2003).

36. *See* Walter, *supra* note 21, at 90.

37. *See* SOLIS, *supra* note 24, at 200.

38. Geyer, *supra* note 1, at 124-25.

39. *Id.* at 124–58.

40. Mark Von Hagen, *People's War: The German Debate about a Levée en Masse in October 1918*, in THE PEOPLE IN ARMS, *supra* note 35, at 187–88.

41. *See* Solis, *supra* note 24, at 200.

existed during a portion of the conflict. Evidencing its contemporary relevance, the Trial Chamber concluded that, for a brief period of time, the situation in and around Srebrenica in 1992 was characterized as a *levée en masse*.[42] More recently, in the 2008 armed conflict between Russia and Georgia over the autonomous and *de jure* demilitarized region known as South Ossetia,[43] the *New York Times* reported, in part, that:

> As swaths of the country fell before Russian troops, it was not only the army that rose in its defense but also regular citizens . . . . [Two young Georgian men] hoped to join the fight . . . despite the fact neither had served in the military . . . . [They were] part of a group of dozen civilians, some in camouflage and some wearing bullet-proof vests, who said they were there to defend the city from Russian attack. . . . "Many of them now think it is the last chance to defend their homeland." Ms. Lagidze said. "It comes from the knowledge that the army is not enough and every man is valuable."[44]

---

42. Prosecutor v. Naser Orić, IT-03-68-T, Judgment, ¶¶ 135–36 (Int'l Crim. Trib. for the former Yugoslavia June 30, 2006). Those paragraphs provide as follows:

> 135. From its inception, the [Army of Bosnia and Herzegovina] sought to provide its members with means of identification such as uniforms, badges and insignia. In the Srebrenica area, however, with the exception of the members of the 16th East Bosnian Muslim Brigade ("16th Muslim Brigade") led by Nurif Rizvanović, very few individuals possessed a complete uniform in 1992 and 1993. Before and after the arrival of this brigade in the area in early August 1992, most Bosnian Muslim fighters wore makeshift or parts of [Yugoslav People's Army] uniforms. To make up for the lack of adequate clothing, civilians also sometimes wore parts of uniforms. There is evidence indicating that during some attacks, fighters wore coloured ribbons around their heads or arms for identification purposes amongst themselves. Apart from these disparate uniforms and ribbons, fighters did not wear fixed distinctive emblems recognizable at a distance.
>
> 136. The Trial Chamber comes to the conclusion that while the situation in Srebrenica may be characterized as a *levée en masse* at the time of the Serb takeover and immediately thereafter in April and early May 1992, the concept by definition excludes its application to long-term situations. Given the circumstances in the present case, the Trial Chamber does not find the term *levée en masse* to be an appropriate characterization of the organizational level of the Bosnian Muslim forces at the time and place relevant to the Indictment.

43. Eneken Tikk, Kadri Kaska, Kristel Runnimeri, Mari Kert, Anna-Maria Taliharm & Lis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified* 4 (2008), *available at* http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

44. SOLIS, *supra* note 24, at 200 (citing Nicholas Kulish & Michael Schwirtz, *Sons Missing in Action, If Indeed They Found It*, NEW YORK TIMES, Aug. 13, 2008, at A14).

As it is extremely likely that in future conflicts there will again be civilian fighting forces that spontaneously form to defend their homeland, understanding both the historical context and legal definition of *levée en masse* is important. The concept of *levée en masse* remains a viable contemporary combatant status as various modern examples, most notably in the Balkans War and the Russian invasion of Georgia, clearly illustrate. Many military manuals and legal scholars are cognizant of the historical relevance and modern importance of the concept and continue to stress the validity of delineating *levée en masse* participants as combatants under the law of armed conflict.[45]

III. THE LAW OF ARMED CONFLICT AND LEVÉE EN MASSE: RECOGNIZING AND REGULATING THE REALITIES OF WAR

A *levée en masse* is a unique and limited battlefield categorization available only during a portion of a declared war or international armed conflict.[46] The Third Geneva Convention of 1949 explicitly entitles participants of *a levée en masse*, upon capture, to prisoner-of-war status.[47] Qualifying for prisoner-of-war status means an individual may gain combatant status,[48] in contrast to

45. *See generally* PRACTICE, *supra* note 27, at 2546–50.

46. In the four 1949 Geneva Conventions, Common Article 2 states, in part, that "the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them." *See, e.g.*, GC III, *supra* note 24, art. 2. Additionally, "[t]he Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance." *Id.* Thus, the Third Geneva Convention, including provisions concerning *levée en masse*, is triggered in the event of an international armed conflict, declaration of war, or occupation. *Id. Levée en masse* as a status does not apply during a non-international armed conflict as it is not provided for in Common Article 3 of the Geneva Conventions. *Id.*, art. 3; TALLINN MANUAL, *supra* note 15, at 102 (noting that a *levée en masse* does "not apply to non-international armed conflict").

47. *See* GC III, *supra* note 24, art. 4(A)(6).

48. "Combatants are generally defined as anyone engaging in hostilities in an armed conflict on behalf of a party to the conflict" and fall "under the definition given in Geneva Convention III for those entitled to Prisoner of War status." INTERNATIONAL & OPERATIONAL LAW DEPARTMENT, THE JUDGE ADVOCATE GENERAL'S LEGAL CENTER & SCHOOL, U.S. ARMY, LAW OF ARMED CONFLICT DESKBOOK 134 (2010)[hereinafter DESKBOOK]. Article 4(A) of the Third Geneva Convention lists four categories of combatant. *See* GC III, *supra* note 24, art. 4(A)(1)–(3), (6). Article 4(A)(6), one of the explicit combatant categories, defines *a levée en masse* as: "Inhabitants of a non-occupied territory,

being defined as an unlawful combatant[49] or civilian.[50] Combatant status, which only exists in international armed conflicts and declared wars,[51] allows *levée en masse* participants to kill and wound without penalty, provided the privilege is not abused by unlawful battlefield acts.[52] As combatants, *levée en masse* participants are allowed to be lawfully attacked,[53] and as noted above,

---

who on the approach of the enemy spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war." More generally, combatants fall into two alternative categories: (1)members of the armed forces of a belligerent party (except medical and religious personnel) even if their specific task is not linked to active hostilities; and (2) any other person taking an active part in hostilities. DINSTEIN, *supra* note 20, at 27.

49. The law of armed conflict does not use the term "unlawful combatant" or "unprivileged belligerent." However, these terms have become workable references to those who engage in combat without meeting the combatant criteria listed in Article 4 of the Third Geneva Convention. *See generally* SOLIS, *supra* note 24, at 206–11 (discussing the history of the terms, criticism of the concept and the negative consequences of being an unlawful combatant); DESKBOOK, *supra* note 48, at 96–97.

50. Despite the obvious significance of distinguishing between combatants and civilians on the battlefield, the Geneva Conventions do not define the term "civilians." However, the *Commentary* to Additional Protocol I states that "the principle protection of the civilian population is inseparable from the principle of distinction which should be made between military and civilian persons," therefore "it is essential to have a clear definition of each of these categories." COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949, at 610 (Yves Sandoz et al. eds., 1987). As a result, Additional Protocol I goes on to specifically define a civilian as "any person who does not belong to one of the categories referred to in Article 4(A)(1), (2), (3) and (6) of the Third Geneva Convention and in Article 43 of this Protocol." Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict art. 50(1), June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I]. Those listed in Article 4(4) and (5) (examples include journalist and others that accompany the armed force) maintain their civilian status, but are afforded the special status as a prisoner of war if captured.

It is important to note that the United States has not ratified Additional Protocol I, but finds many portions reflect customary international law. *See generally* Michael J. Matheson, *Remarks on the United States Position on the Relation of Customary International Law to the 1977 Protocols Additional to the 1949 Geneva Conventions,* 2 AMERICAN UNIVERSITY JOURNAL OF INTERNATIONAL LAW & POLICY 419 (1987).

51. *See* JEAN-MARIE HENCKAERTS & LOUISE DOSWALD-BECK, 1 CUSTOMARY INTERNATIONAL HUMANITARIAN LAW: RULES 11–12, Rule 3 (2005).

51. *See* GREENSPAN, *supra* note 26, at 3.

52. SOLIS, *supra* note 24, at 42.

53. A.P.V. ROGERS, LAW ON THE BATTLEFIELD 8 (2d ed. 2004).

afforded prisoner-of-war status upon capture.[54] However, "[t]he permissible window of opportunity for the raising of and participation in a *levée* is extremely narrow."[55] The *Commentary* to the Third Geneva Convention acknowledges that a *levée en masse* can only exist for a short period of time as it is a spontaneous uprising and will eventually take on structure or no longer be in unoccupied territory.[56] Thus, if the *levée en masse* continues beyond the initial invasion, "the authority commanding the inhabitants who have taken up arms, or the authority to which they profess allegiance, must either replace them by sending regular units, or must incorporate them in its regular forces."[57]

Recognizing the temporal nature of a *levée en masse*, participants receive combatant status under relaxed conditions and are exempt from two of the four conditions required of other irregular troops.[58] These other irregular troops, whether members of militia, other volunteer corps or those of organized resistance belonging to a party to a conflict, may be considered combatants and receive the resultant privileges, provided they fulfill the following four conditions:

> (a) that of being commanded by a person responsible for his subordinates;
> (b) that of having a fixed distinctive sign recognizable at a distance;
> (c) that of carrying arms openly;
> (d) that of conducting their operation in accordance with the laws and customs of war.[59]

In contrast, *levée en masse* participants are neither required to be commanded by a person responsible for his subordinates nor wear a fixed dis-

54. *See* GC III, *supra* note 24, art. 4(A)(6). The United States law of land warfare field manual states that "[s]hould some inhabitants of a locality thus take part in its defense, it might be justifiable to treat all the males of military age as prisoners of war." U.S. Department of the Army, FM 27-10, The Law of Land Warfare 28 (Change 1, 1976)[hereinafter FM 27-10]. The manual goes on to say that "[e]ven if inhabitants who formed the *levée en masse* lay down their arms and return to their normal activities" they may still be made prisoners of war. *Id.*

55. Crawford, *supra* note 28, at 13.

56. COMMENTARY, III GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 68 (Jean S. Pictet ed., 1960)[hereinafter COMMENTARY, GC III].

57. *Id. See also* Crawford, *supra* note 28, at 13.

58. *See* GREENSPAN, *supra* note 26, at 62; GC III, *supra* note 23, art. 4(A)(2).

59. GC III, *supra* note 24, art. 4(A)(6).

tinctive sign to receive combatant status.[60] Given that a *levée en masse* is a spontaneous, unorganized movement[61] acting under emergency conditions to desperately defend a nation,[62] it is understandable that the inhabitants of the territory will not have sufficient time to organize into units and have distinctive signs. Though justifiable, these relaxed combatant qualification standards significantly diminish the ability of an armed force fighting a *levée en masse* to distinguish between a civilian and a combatant.[63] Thus, "the requirement of carrying arms 'openly' is of special significance and has a more precise implication"[64] for both the *levée en masse* participants and their adversaries. For those fighting a *levée en masse*, the only distinguishing characteristic between a protected civilian and a combatant, and, therefore, who can be lawfully attacked, is the open carrying of arms. For *levée en masse* participants, "this requirement is in the interest of [the] combatants themselves who must be recognizable in order to qualify for treatment as prisoners of war."[65] Recognizing both the realities of a *levée en masse* and the criticality of protecting civilians, the law of armed conflict places singular emphasis on the essential need for those choosing to participate in a spontaneous uprising to "carry arms visibly."[66]

The concept of *levée en masse*, though narrower and more specific than originally espoused during the French Revolution, remains a contemporary combatant category.[67] Yet, as the law of armed conflict struggles to maintain the balance between military necessity and humanity in modern warfare,[68] particularly in cyber conflicts, the viability of a *levée en masse* must be questioned. A spontaneous uprising of a nation's citizenry to defend the unoccupied portions of their territory is a far different paradigm than a cyber mobilization.

---

60. *See id.*; GREENSPAN, *supra* note 26, at 62. *See also* FM 27-10, *supra* note 54, at 28 (stating "[i]f the enemy approaches an area for the purpose of seizing it, the inhabitants, if they defend it, are entitled to the rights of regular combatants as a *levée en masse* although they wear no distinctive sign").

61. GREENSPAN, *supra* note 26, at 62.

62. SOLIS, *supra* note 24, at 201.

63. *See supra* note 48 for membership criteria for a *levée en masse.*

64. COMMENTARY, GC III, *supra* note 56, at 68.

65. *Id.*

66. *Id.*

67. *See* Crawford*, supra* note 28, at 13 (stating "[a]s the concept of *levée en masse* has evolved and developed over the decades, it has become a far narrower concept than originally espoused during the French Revolution.").

68. *See generally* Reeves & Barnsby, *supra* note 6, at 16–18 (discussing the difficulties of maintaining a balance between these countervailing interests in modern warfare).

IV. LEVÉE EN MASSE IN CYBER WARFARE: TECHNOLOGY MEETS TRADITION—AN ANALYSIS

The *Tallinn Manual*, the non-binding, yet authoritative interpretation of how the existing law of armed conflict applies to cyber warfare, addresses many critically important issues.[69] Of particular note is the *Manual*'s Rule 27, which states that "in an international armed conflict, inhabitants of an unoccupied territory who engage in cyber operations as part of a *levée en masse* enjoy combatant immunity and prisoner of war status."[70] In validating the notion of a cyber *levée en masse*, the international group of experts acknowledges the problematic nature of applying the concept to cyber warfare by highlighting various unanswered and troubling questions in the commentary to Rule 27.[71] Additionally, the experts were "divided as to whether the privileges associated with the *levée en masse* concept apply to a civilian population countering a massive cyber attack, the affects of which are comparable to those of a physical invasion by enemy forces."[72] Unable to come to a consensus, a majority of the experts decided that the concept is only applicable when there is a physical invasion of national territory. Put differently, a cyber *levée en masse* is only possible when responding to a traditional invasion of territory by a conventional force.[73] It is not permitted in the face of an attack that consists only of cyber operations.

The *Tallinn Manual*'s preservation, yet conservative treatment, of the concept of *levée en masse* is consistent with the belief that

> [t]he development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them.[74]

---

69. TALLINN MANUAL, *supra* note 15, at 1.

70. *Id.* at 102.

71. *See id.* at 102–03, cmt. to Rule 27(discussing various problems with the concept of a cyber *levée en masse*).

72. *Id.* at 103.

73. *Id.*

74. *See* THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 9 (2011), *available at*

Though this approach has merit, there is an equally compelling argument that it is critical to resolve the problems associated with extending the *levée en masse* concept to cyberspace. At the forefront of these problems is the inability to distinguish between a cyber *levée en masse* combatant and a protected civilian. As a *levée en masse* is a spontaneous uprising, inhabitants are expected to be participants in impulsively organized groups[75] that are only distinguishable as combatants by the open and visible carrying of arms.[76] There is no confusion as to what "arms" may mean in the context of a traditional *levée en masse*, as conventional weapons such as rifles, pistols and similar armaments are clearly contemplated.[77] *Levée en masse* participants, with no distinctive signs recognizable from a distance, are therefore expected to ostensibly carry traditionally recognized weapons since this is the only external display advertising their combatant status.[78]

This singular distinction requirement is not possible in a cyber war where the weapons are computers. Though a computer at times may be construed as a "weapon,"[79] simple possession cannot be interpreted to be indicative of combatant activity. As the *Tallinn Manual* notes, "even if [computers] qualify as weapons, the requirement to carry arms openly has little application in the cyber context,"[80] thus verifying that this most important of distinguishing characteristics is nonexistent. Without a visible weapon, there is no meaningful way to distinguish a theoretical cyber *levée en masse* from the civilian population.

The irrelevance of geography in cyberspace and the limited cyber expertise of a territory's population both further contribute to this significant distinction problem.[81] Cyber warfare's attractiveness is partially due to the abil-

---

http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

75. GC III, *supra* note 24, art. 4(A)(6).

76. *See* COMMENTARY, GC III, *supra* note 56, at 67–68; *supra* text accompanying notes 61–66.

77. *See* COMMENTARY, GC III, *supra* note 56, at 61(discussing the requirement of carrying arms openly, referring to weapons such as a hand grenade or a revolver).

78. *See id.* at 61, 67.

79. The *Tallinn Manual* defines a cyber weapon as "cyber means of warfare that are by design, use, or intended use capable of causing either (i)injury to, or death of, persons; (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as an attack." TALLINN MANUAL, *supra* note 15, at 141–42.

80. *Id.* at 100.

81. *Id.*

ity of an individual to effectively organize a cyber campaign,[82] while remaining safely anonymous from an undisclosed location.[83] "Territory" is a non-factor in cyber warfare; the location of the cyber attacker, the digital infrastructure transmitting the attack and the target are widely dispersed and not bound by an occupied/unoccupied paradigm.[84] The territorial component that helps define a *levée en masse*, specifically that the uprising will remain restricted to "unoccupied territory," thus does not comport with the realities of cyber warfare.[85] Further, "the means and expertise necessary to engage effectively in cyber operations may be relatively limited in the population," eliminating the possibility of a mass uprising.[86] When comparing the historical narrative of a *levée en masse*—large numbers of armed citizens spontaneously coalescing in order to repel invaders—to the cyber version—technically skilled citizens discreetly using their computers from an undisclosed location to attack invaders[87]—the stark differences highlight the flaws in trying to apply the traditional concept in the cyber domain. A small dispersed group of citizens not limited to simply protecting unoccupied territory, but conducting cyber operations possibly deep inside enemy territory, is contrary to the conceptual underpinnings of a *levée en masse*.[88] Given the unlikely ability of a population to conduct a mass cyber uprising or for technically proficient citizens to limit a cyber attack to those forces "at the front,"

---

82. Korns & Kastenberg *supra* note 11, at 70.

83. *See*, *e.g.*, Kelly Gables, *Cyber-Apocalypse Now: Securing the Internet against Cyberterrorism and Using Universal Jurisdiction as a Deterrent*, 43 VANDERBILT JOURNAL OF TRANSNATIONAL LAW 57, 57 (2010) (discussing the unlimited reach of terrorist activity over the Internet).

84. Illustrating the irrelevance of geographic borders in cyberspace, author P.W. Singer noted when describing a Hezbollah cyber assault on Israel in 2006 that the attack "originally appeared to come from a small south Texas cable company, a suburban Virginia cable provider and web-hosting servers in Delhi, Montreal, Brooklyn, and New Jersey," while in actuality "these all had actually been 'hijacked' by Hezbollah hackers." P.W. SINGER, WIRED FOR WAR 264 (2009).

85. *See* Korns & Kastenberg *supra* note 11, at 70 ("Existing international laws of war are generally based on the notion of 'borders' in that these laws primarily govern conflicts between nation-states with recognized geographic boundaries. This construct is fundamentally weak in addressing borderless, nonstate actor participation in cyber conflict where individuals organize their own cyber campaigns.").

86. TALLINN MANUAL, *supra* note 154, at 103.

87. *Id.* (discussing how a cyber *levée en masse* may theoretically form).

88. *Id.* (noting that historically, *levée en masse* did not "contemplate military operations deep inside enemy territory, it is questionable whether individuals launching cyber operations against enemy military objectives other than the invading forces can be considered a *levée en masse*").

neither significant population participation nor geography can be considered distinguishing characteristics of a theoretical cyber *levée en masse*.

A cyber *levée en masse* is simply an unworkable notion whose continued viability increases the likelihood of greater indiscriminate targeting of the civilian population. Preserving a combatant category that lacks any distinctive indicators creates a murky environment[89] in which civilians may easily be mistaken for combatants.[90] One of the primary purposes of the law of armed conflict is to protect civilians,[91] as explicitly articulated in the principle of distinction,[92] thus "it is of the utmost importance that all feasible measures be taken to prevent the exposure of the civilian population to erroneous or arbitrary targeting."[93] In contrast, a cyber *levée en masse* combatant category increases "confusion and uncertainty as to the distinction between legitimate military targets and persons protected against direct attack"[94] and therefore acts in direct opposition to this well-established principle. Whether due to the irresolvable distinction problem, or because of a complete dissimilarity between a traditional *levée en masse* and the cyber variant, it is untenable to maintain this combatant category in cyber warfare.

A more reasonable solution, which both enforces the principle of distinction and protects assemblages of cyber participants, is to require these groups to comply with a modified version of criteria required for other irregular troops, such as militias, volunteer corps or organized militia movements.[95] Because the existing criteria for traditional irregular troops to gain combatant status include "carrying arms openly,"[96] strict compliance with this requirement is not possible in any cyber context.[97] But unlike the concept of *levée en masse*, which places special significance on carrying arms

89. Distinguishing parties to the conflict in cyberspace is recognized as extraordinarily difficult. *See* Korns & Kastenberg *supra* note 11, at 70.

90. *See* Melzer, *supra* note 13, at 833.

91. *See* ICRC Interpretive Guidance, *supra* note 8, at 4 (stating that "the protection of civilians is one of the main goals of international humanitarian law").

92. The principle of distinction states that "in order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives. . . ." AP I, *supra* note 50, art. 48.

93. ICRC Interpretive Guidance, *supra* note 8, at 7.

94. Melzer, *supra* note 13, at 833.

95. *See* GC III, *supra* note 24, art. 4(A)(2); text and accompanying notes 56-57(listing the four criteria for irregular troops to gain combatant status).

96. *See* GC III, *supra* note 24, art. 4(A)(2)(c)(noting that the third cumulative condition for combatant status is "that of carrying arms openly").

97. TALLINN MANUAL, *supra* note 15, at 100.

openly,[98] this requirement is not the only manner in which to recognize an irregular troop as a combatant. Carrying arms openly is of diminished importance in the irregular troop combatant category as other external signs, in particular "being commanded by a person"[99] and "having a fixed distinctive sign recognizable at a distance," help distinguish these groups from civilians.[100] Though unfeasible in the context of a *levée en masse*,[101] eliminating this requirement as a qualification for an irregular cyber troop is a possibility due to the alternative distinguishing criteria.

Additionally, the remaining militia, volunteer corps and organized resistance movement membership criteria more accurately reflect current cyber war conditions than does the notion of a *levée en masse*. Limited technical expertise, coupled with the global scope of the cyber domain,[102] makes a spontaneous, geographically restricted mass cyber uprising an unrealistic, or, at best, extremely remote possibility.[103] A more likely scenario is a group of cyber-capable citizens, who possess the requisite technical expertise, inconspicuously organizing to engage an invading force in cyber warfare.[104] Organization of the cyber-capable citizens and the unrestricted use of cyberspace to affect the invading force are analogous to irregular troops being under command and allowed to operate "in or outside their own territory,

---

98. *See* COMMENTARY, GC III, *supra* note 56, at 67–68; *supra* text accompanying notes 62–64.

99. "The condition of being commanded by a person responsible for subordinates is best understood as an aspect of the requirement that the group be 'organized.'" TALLINN MANUAL, *supra* note 15, at 98. As noted in the *Manual*, a group that is organized solely over the Internet will not qualify as an organized armed group as they will "have difficulty establishing that they are acting under a responsible commander" or "subject to an internal disciplinary system capable of enforcing compliance with the Law of Armed Conflict." *Id.* Therefore, physical organization is required to gain combatant status. *See id.*

100. GC III, *supra* note 24, art. 4(A)(2)(a)(b).

101. The *Commentary* to the Third Geneva Convention, recognizing the critical importance of a *levée en masse* visibly carrying their weapons in order to be distinguished as combatants explains the difference between carrying arms "openly" and carrying them "visibly." COMMENTARY, GC III, *supra* note 56, at 61.

102. TALLINN MANUAL, *supra* note 15, at 258–60 (defining cyberspace broadly and describing the Internet as "global").

103. "At the core" of the *levée en masse* concept is "the notion of spontaneity and brevity." Crawford, *supra* note 28, at 13. Gathering together those who have the technical expertise to conduct a concerted cyber attack will take effort and will unlikely comport to the understanding of "spontaneous."

104. *See* Korns & Kastenberg, *supra* note 11 at 70 (discussing the "the growing trend of cyber conflict between nations and ad hoc assemblages").

even if [that] territory is occupied."[105] Some may question the likelihood of a cyber group wearing "a fixed distinctive sign recognizable at a distance";[106] however, since there are only a limited number of distinctive characteristics available in the cyber context, there is "no basis for deviating from" this general requirement if the group is to be afforded combatant immunity and prisoner-of-war status.[107] Similarly, as compliance with the law of armed conflict is a universal requirement for maintaining combatant status, this criterion obviously remains unchanged. For those individuals or loosely affiliated groups that choose to participate in cyber operations without meeting the modified membership criteria for a militia, volunteer corps or an organized resistance movement, they may be taking a direct part in hostilities.[108] In doing so, they risk divesting themselves of their civilian protections, thereby becoming subject to targeting and prosecution for belligerent acts.[109]

"When bombs and bullets fly, identification of warring parties is relatively easy; but not so for cyber activities,"[110] thus the need for greater clarity in defining a combatant in cyber warfare. Despite this necessity, the *Tallinn Manual* preserves the idea of a cyber *levée en masse*, thus maintaining a combatant status that is indistinguishable from the civilian population. In doing so, it ignores the contemporary realities of cyber warfare. This is dangerous and requires a workable alternative that provides the same opportunities for assemblages of cyber participants during the traditional period of a *levée en masse*. The membership criteria for the militia, volunteer corps or an organized resistance movement, modified for the cyber context, fills this need as it creates a combatant category for cyber capable citizens without the irresolvable issues of a *levée en masse*.

---

105. GC III, *supra* note 24, art. 4(A)(2).

106. *Id.*, art. 4(A)(2)(b).

107. Though there is "no basis for deviating from this general requirement for those engaged in cyber operations," there are questions as to whether there are exceptions. *See generally* TALLINN MANUAL, *supra* note 15, at 99. Regardless of whether customary international law recognizes exceptions to this requirement in regards to a traditional militia, volunteer corps or organized resistance movements, in the context of cyber war this requirement has greater importance due to the limited number of distinctive characteristics available.

108. *See* AP I, *supra* note 50, art. 51(3).

109. *See generally* Michael N. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, 1 HARVARD NATIONAL SECURITY JOURNAL 1 (2010) (discussing the consequences of a civilian taking a direct part in hostilities).

110. Korns & Kastenberg *supra,* note 11, at 70.

V. CONCLUSION & RECOMMENDATION

Levée en masse, where "inhabitants of a non-occupied territory, on the approach of the enemy spontaneously take up arms to resist the invading forces, without having time to form themselves into regular armed units," provides both prisoner-of-war protections and combatant immunity to individual participants if they "carry arms openly and respect the laws and customs of war."[111] The requirements of spontaneous mass uprising, protecting non-occupied territory and "carrying arms openly" have special significance as these are essentially the only distinguishing characteristics of a *levée en masse*.[112] Because cyberspace is a borderless domain, where computers are the weapons and groups discreetly coalesce,[113] the concept of *levée en masse* becomes an unworkable anachronism whose application diminishes various protections afforded both civilians and conflict participants in armed conflicts.[114] Rather than forcibly applying a concept that is incongruous in this new domain, a more practical solution is to eliminate *levée en masse* as a combatant category in cyber conflicts and instead require all assemblages of cyber participants, either ad hoc or pre-existing, to generally comply with the criteria that define militias, volunteer corps or organized resistance movements.[115]

In contrast to *levée en masse*, this combatant category eliminates the importance of territorial occupation[116] and helps distinguish individual computer attacks from an organized cyber operation. Admittedly, this is not a perfect solution since computers are the exclusive tool used in cyberspace, and one of the qualifying conditions for militias, volunteer corps or orga-

111. GC III, *supra* note 24, art. 4(A)(6).

112. COMMENTARY, GC III, *supra* note 56, at 68.

113. QDR, *supra* note 4, at ix; Korns & Kastenberg *supra* note 11, at 70 (stating "international laws of war . . . are fundamentally weak in addressing borderless, nonstate actor participation in cyber conflict where individuals organize their own cyber campaigns").

114. *See*, *e.g.*, *supra* text accompanying notes 89–94 for a discussion on how applying the concept of *levée en masse* in a cyber conflict potentially increases indiscriminate targeting of civilians and confuses combatant status.

115. GC III, *supra* note 24, art. 4(A)(2). The following four conditions must be fulfilled to qualify for this provision: "(a) that of being commanded by a person responsible for his subordinates; (b) that of having a fixed distinctive sign recognizable at a distance; (c) that of carrying arms openly; (d) that of conducting their operations in accordance with the laws and customs of war."

116. *Id.*, art. 4(A)(2)(noting that members of this combatant category may operate "in or outside their own territory, even if [that] territory is occupied.").

nized resistance movements includes the requirement to "carry arms openly."[117] However, unlike a *levée en masse*, this category greatly diminishes the importance of "carry[ing] arms openly" by providing a variety of other criteria to help distinguish combatants from civilians.[118] If extended to include spontaneous cyber uprisings, the carrying arms openly requirement could be eliminated, while participants could remain in compliance with the principle of distinction through other means.[119] For those cyber assemblages not complying with the conditions that would categorize participants as members of a militia, volunteer corps or organized resistance movement as those apply to all other conflicts, individuals retain their civilian status until taking a direct part in hostilities.[120] Eliminating a possible *levée en masse* in cyber conflict and emphasizing the criteria, albeit slightly modified, defining militias, volunteer corps or organized resistance movements helps demarcate the line between a combatant and civilian in the ambiguous cyber war environment.

The impracticality of applying the concept of *levée en masse* in cyberspace, and the subsequent need to modify criteria for the irregular troop combat-

117. *Id.*, art. 4(A)(2)(c).

118. For example, a "fixed distinctive sign," command structure and belonging to a party to the conflict. *Id.*, art. 4(A)(2)(c).

119. "In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives. . . ." AP I, *supra* note 50, art. 48. The distinction requirement also applies in non-international armed conflict. *See* Protocol Additional to the Geneva Conventions of August 1949, and Relating to the Protection of Victims of Non-International Armed Conflict art. 13, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II] (stating "civilians shall enjoy the protection afforded by this part, unless and for such time as they take a direct part in hostilities"); SOLIS, *supra* note 24, at 254 (discussing the applicability of the principle of distinction in all conflicts); Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC 'Direct Participation in Hostilities' Interpretive Guidance*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLICY 641, 646 (2010) ("[c]ompliance with the distinction principle is required of all participants in warfare regardless of whether they fight for state armed forces or a non-State 'organized armed group'").

120. "Civilians shall enjoy the protection afforded by this part, unless and for such time as they take a direct part in hostilities. AP I, *supra* note 50, art. 51(3); AP II, *supra* note 119, art. 13. There is much debate concerning what constitutes "a direct part in hostilities" in not only the cyber context, but in traditional forms of warfare. *Compare* ICRC Interpretive Guidance, *supra* note 8, at 5–6 ("The *Interpretive Guidance* provides a legal reading of the notion of 'direct participation in hostilities' with a view to strengthening the implementation of the principle distinction.") *with* Watkin, *supra* note 119, at 641 *and* Schmitt, *supra* note 109, at 5 (criticizing the *Interpretive Guidance* recommendations). Though this particular issue is outside the purview of this paper, it again illustrates the difficulties faced when attempting to conform the existing law of armed conflict to cyber warfare.

ant category, highlights the immense challenge of regulating cyber warfare with the existing law of armed conflict. Cyberspace—"a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the Internet and telecommunication networks"[121]—is quickly becoming a decisive battleground in warfare.[122] National armed forces, more specifically, technologically advanced militaries, are highly dependent upon their information networks for command and control, intelligence, logistics and weapon technology.[123] The result of this dependency is that "modern armed forces simply cannot conduct high-tempo, effective operations without . . . assured access to cyberspace."[124] However, access to cyberspace is not limited to technologically advanced militaries as State actors with scarce resources, non-State armed groups or even individuals[125] are capable of cyber participation from almost any location.[126] Ease of access, widespread computer sophistication and cheap "hacker tools" allow this broad range of actors to create a staggering number of vulnerabilities for a cyber-reliant military.[127] Further, the anonymity and borderless nature of cyberspace incentivizes hostile actors to exploit these vulnerabilities,[128] making computer attacks an attractive method of warfare.[129] Cyber warfare, with all its concomitant legal issues is thus

---

121. *See* QDR, *supra* note 4, at 37.

122. *Id.*

123. *Id.*

124. *Id.*

125. *See, e.g.,* Lee Ferran, *Former CIA Counter-Terror Chief: Al Qaeda Will Go Cyber*, (ABC Nightly News television broadcast Aug. 4, 2011), http://abcnews.go.com/Blotter/cia-counter-terror-chief-al-qaeda-cyber/story?id=14224256 (noting that Al-Qaeda has specifically called for cyber attacks as they can be done remotely and individually); Duncan Gardham, *Terrorists are harnessing hi-tech communications, government warns*, TELEGRAPH (July 12, 2011), http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/8633311/Terrorists-are-harnessing-hi-tech-communications-government-warns.html (discussing Al-Qaeda's guidance for individuals to act independently as they conduct "cyber jihad.").

126. *See*, *e.g.*, SINGER, *supra* note 84, at 264.

127. *See* QDR, *supra* note 4, at 37.

128. *See*, *e.g.*, *Global Hacking Network Declares Internet War on Syria,* REUTERS (Nov. 30, 2012), http://in.reuters.com/article/2012/11/30/syria-crisis-internet-anynymous-idINDEE8AT0C320121130 ("Global hacking network Anonymous said it will shut down Syrian government websites around the world in response to a countrywide Internet blackout believe aimed at silencing the opposition to President Bashar al-Assad.").

129. *See U.S. Cyber Command: Organizing for Cyberspace Operations: Hearing Before the H. Comm. on Armed Services,* 111th Cong. 1 (2010) (statement of Rep. Skelton, Chairman, H. Comm. on Armed Services)("[U.S] information systems face thousands of attacks a day

becoming a regular occurrence as historically marginalized actors are drawn to the unprecedented opportunities—and limited risks—presented in the cyber domain.[130]

As cyber warfare becomes common, the international community cannot continue to rely on a static version of the existing law of armed conflict to resolve the "wicked" problems inherent in the "fifth domain."[131] Only by looking beyond *lex lata*,[132] or how the existing law of armed conflict applies in cyber warfare,[133] and exploring *lex ferenda*,[134] or what the law in cyberspace should be, will States begin to develop solutions to the legal ambiguity that permeates cyber warfare and gain the clarity needed for operating in cyberspace. In modern warfare the "pace of change continues to accelerate,"[135] often straining the ability of the law of armed conflict to regulate contemporary conflicts. No emerging form of warfare creates more ambiguous legal questions than does cyber war, thus posing a great threat to the continued vitality of the law of armed conflict. Just as global militaries are adapting their doctrine, tactics and force structure to address the realities of cyberspace,[136] innovations in the law are necessary for effective regulation of this new domain. Addressing this threat is of paramount importance, as proactively keeping the law of armed conflict relevant maintains the delicate bal-

---

from criminals, terrorist organizations, and more recently from more than 100 foreign intelligence organizations.").

130. *See id.* (statement of Rep. Skelton, Chairman, H. Comm. on Armed Services) ("[U.S] information systems face thousands of attacks a day from criminals, terrorist organizations, and more recently from more than 100 foreign intelligence organizations.").

131. Along with land, sea, air and space, cyberspace is considered the fifth domain of warfare. *See War in the Fifth Domain,* ECONOMIST, July 3, 2010, at 25, *available at* http://www.economist.com/node/16478792. *See also* QDR, *supra* note 4, at 37 ("Although it is a man-made domain, cyberspace is now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air, and space.").

132. *Lex lata* is defined as "what the law is." *See* J. Jeremy Marsh, Lex Lata *or* Lex Ferenda*? Rule 45 of the ICRC Study on Customary International Humanitarian Law*, 198 MILITARY LAW REVIEW 116, 117 (2008).

133. TALLINN MANUAL, *supra* note 15, at 5. The *Manual* notes that its purpose is to explain the "law currently governing cyber conflict" and "does not set forth *lex ferenda*, best practices, or preferred policies." *Id.*

134. *Lex ferenda* is defined as "what the law should be." *See* Marsh, *supra* note 132, at 117.

135. QDR, *supra* note 4, at iii.

136. *See*, *e.g.*, QDR, *supra* note 4, at 62 ("rising complexity in sea, air, space and cyberspace domains pose new security challenges that require innovative adjustments to our defense posture."). *See also* Reeves & Barnsby, *supra* note 6, at 17 (discussing the adverse implications of a nation not recognizing new strands of warfare).

ance between military necessity and humanity, which ensures the primacy of the law remains unquestioned.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Precision Air Warfare and the Law of Armed Conflict

Christopher J. Markham
Michael N. Schmitt

89 INT'L L. STUD. 669 (2013)

Volume 89 2013

Precision Air Warfare and the Law of Armed Conflict

Christopher J. Markham[*]
Michael N. Schmitt[**]

I. INTRODUCTION

Precision attacks dominate contemporary aerial warfare. The centrality of precision operations derives not only from their military utility, but also from the international community's evolving expectations with respect to the avoidance of collateral damage. As technological developments in the field proceed apace, the emphasis on precision can only be expected to grow.

This article examines the synergistic relationship between precision airstrikes and the law of armed conflict. It defines precision, briefly reviews the history of its rise to prominence in aerial warfare, examines the application of the law of armed conflict to precision attacks and considers several new precision weapon systems. In sum, the article explores both how the

* First Lieutenant, United States Marine Corps; Fellow, International Law Department, United States Naval War College.

** Chairman, International Law Department, United States Naval War College; Honorary Professor, Exeter University (UK). The views expressed in this article are those of the authors in their personal capacity.

law of armed conflict governs the use of precision capabilities and how advances in precision capabilities are likely to shape the law of armed conflict.

II. THE DEFINITION OF "PRECISION" AND A BRIEF HISTORY

A. "Precision" Defined

"Precision" refers to the "ability to locate and identify a target, strike it accurately in a timely fashion, and determine whether desired effects have been achieved or restrike is needed."[1] In discussing precision, many scholars address only accuracy. "Accuracy" refers to a weapon's capacity to strike a specific aimpoint[2] and is an integral aspect of any precision airstrike.

But accuracy alone is insufficient to render a strike "precise." Precision is just as dependent on command, control, communications, computers, intelligence, surveillance, and reconnaissance (known as C4ISR) capabilities. In fact, on a complex battlefield, ISR,[3] not accuracy, often proves the key aspect of a precision airstrike. For example, during Operation Enduring Freedom U.S. aircraft twice mistakenly attacked International Committee of the Red Cross warehouses.[4] Weapons accuracy played no role in the attacks—the missiles landed exactly where they were aimed. Instead, the problem was a failure in the targeting process, which is C4ISR driven.

It is likewise important to recognize that the environment in which an airstrike takes place can affect the accuracy of a weapon system and the quality of the associated C4ISR. For instance, nighttime or inclement

1. Michael N. Schmitt, *Precision Attack and International Humanitarian Law*, 87 INTERNATIONAL REVIEW OF THE RED CROSS 445, 446 (2005).

2. An "aimpoint" is "[a] point associated with a target and assigned for a specific weapon impact. [It] may be defined descriptively (e.g., vent in center of roof), by grid reference, or geolocation. More specific classifications of aimpoint include desired point of impact, joint desired point of impact, and desired mean point of impact." Joint Chiefs of Staff, Joint Publication 1-02, DoD Dictionary of Military and Associated Terms (Nov. 8, 2010), as amended through July 15, 2012, http://www.dtic.mil/doctrine/dod_dictionary [hereinafter DoD Dictionary].

3. "[I]ntelligence, surveillance, and reconnaissance" is "[a]n activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function." *Id.*

4. For a discussion of these incidents, see Sean D. Murphy, *Contemporary Practice of the United States Relating to International Law*, 96 AMERICAN JOURNAL OF INTERNATIONAL LAW 247 (2002).

weather limits the effectiveness of certain weapon systems. Fire can diminish the usefulness of infrared equipment and smoke may prevent visual target identification, as was demonstrated during coalition airstrikes in the 1990–1991 Gulf War after Kuwaiti oil wells were set ablaze by Iraqi forces. If a target is heavily defended, an attacker may be forced to launch from a greater-than-optimal weapons release altitude or range or conduct evasive maneuvers that make the launch platform unsteady. And, of course, human error is always possible in the heat of battle.

B. Rise of Precision Airstrikes

Airpower played no significant role in armed conflict until World War I, when it was initially employed for surveillance and reconnaissance; the first aerial attacks took the form of close air support for ground forces. Later in the conflict, belligerents began to use aircraft for strategic strikes, most notably in the zeppelin raids against London.[5] By 1918, the U.S. Air Service and the American Expeditionary Force had drafted a strategic bombing plan which involved "drop[ping] aerial bombs upon commercial centers and the lines of communications in such quantities as will wreck the points aimed at and cut off the necessary supply lines."[6] The war ended before the plan could be executed.

In the aftermath of World War I, most air forces engaged in comprehensive doctrine reviews. The United States, for example, conducted the U.S. Bombing Survey, which concluded that the "successful application of airpower requires a predetermined plan calculated to destroy the enemy's will and war sustaining capability. Achieving this goal requires systematic analysis to determine which targets, if destroyed, would do the greatest damage to the enemy."[7] In a sense, the Bombing Survey argued for what would at the end of the century come to be known as "effects-based operations."[8] Conducting operations to achieve particular results, rather than simply wearing down the enemy's fielded forces, requires that an attacker

5. For an in-depth history of airpower, see STEPHEN BUDIANSKY, AIR POWER: THE MEN, MACHINES, AND IDEAS THAT REVOLUTIONIZED WAR, FROM KITTY HAWK TO GULF WAR II (2004).

6. U.S. Air Force, AF Pamphlet 14-210, Intelligence Targeting Guide, AF Pamphlet 14-210, attachment 2 (Feb. 1, 1998). See this attachment generally for a summary of airpower theory development.

7. *Id.*

8. *See, e.g.*, Joint Chiefs of Staff, Joint Publication 3-60, Joint Doctrine for Targeting, I-1 (Jan. 17, 2002).

deconstruct enemy systems in order to identify those objectives the destruction of which will achieve specific desired effects. Precision makes this possible.[9]

At the time of the U.S. Bombing Survey, the precision technology capable of accomplishing such missions was years from development. During World War II, for example, a B-17 had a circular error probable[10] of roughly 3,300 feet. This meant that at 6,500 feet, approximately 9,000 bombs from 1,500 aircraft would have to be dropped to achieve a high probability of destroying a point target.[11] Complicating matters was the fact that missions often were flown at night and at high altitude to avoid enemy air defenses, thereby further diminishing the precision of the attacks.

Air operations during the Vietnam conflict marked a sea change in precision warfare. A new generation of laser-guided weapons finally enabled a single aircraft to destroy a target in one attack. Since the Vietnam conflict, dramatic technological advances have continued with respect to both precision weapons and C4ISR capabilities. The result has been a sharp rise in the percentage of airstrikes that employ precision systems. For example, precision munitions were used in only 8.8 percent of attacks during Operation Desert Storm (1991).[12] By the initial phases of Operation Enduring

---

9. Michael N. Schmitt, *Effects-Based Operations and the Law of Aerial Warfare*, 5 WASHINGTON UNIVERSITY GLOBAL STUDIES LAW REVIEW 265, 276 (2006).

10. "[C]ircular error probable" is "[a]n indicator of the delivery accuracy of a weapon system, used as a factor in determining probable damage to a target. It is the radius of a circle within which half of a missile's projectiles are expected to fall. Also called CEP." DoD Dictionary, *supra* note 2.

11. Colonel Gary L. Crowder, Chief of Strategy, Concepts, and Doctrine, Department of Defense Air Combat Command, Effects Based Operations Briefing (Mar. 19, 2003), http://www.defenselink.mil/Transcripts/Transcript.aspx?TranscriptID=2067. As another example,

> during Operation Cobra, the breakout from Normandy, U.S. air forces dropped 14,600 500-pound bombs on one German division, destroying 66 tanks and 11 heavy guns. During Operation Desert Storm, the U.S. dropped 9,800 precision-guided munitions, destroying 2,500 tanks, heavy artillery pieces, and armoured personnel carriers—a ratio of bombs to destruction of equipment 50 times greater than in Operation Cobra.

Robert A. Pape, *Hit or Miss: What Precision Air Weapons Do, Precisely*, FOREIGN AFFAIRS, Sept./Oct. 2004, at 162, 163.

12. WILLIAM M. ARKIN ET AL., GREENPEACE, ON IMPACT: MODERN WARFARE AND THE ENVIRONMENT, A CASE STUDY OF THE GULF WAR 78 (1991).

Freedom (2001) and Operation Iraqi Freedom (2003), those figures were at 65 percent and 68 percent, respectively.[13]

Technology has progressed to the point where a basic precision strike capability is within the reach of even less advanced militaries. A prime example is the Joint Direct Attack Munition (JDAM), which is simply an unguided bomb to which a guidance tail kit has been attached. At $22,000 per kit, the JDAM is relatively uncomplicated and cheap.[14] JDAMs are also fairly accurate, allowing for a precision airstrike with a circular error probable of less than twenty feet from as far away as fifteen miles.[15]

Beyond their obvious utility in conventional warfare, precision airstrikes are particularly useful in air campaigns where the objective is not mere attrition of the enemy's armed forces. The best example is compellance (or coercive) warfare, in which the objective is to induce an adversary to engage in, or desist from, particular behavior. NATO adopted this approach during Operation Allied Force, the 1999 air campaign against the Federal Republic of Yugoslavia. The goal of that campaign was to force President Slobodan Milosevic to resume negotiations and end the mistreatment of the Kosovar-Albanian population by his forces.[16] To achieve these objectives, NATO relied on precision airstrikes to attack specific targets, the destruction of which it believed would convince Milosevic to return to the bargaining table and stop the slaughter. The campaign succeeded in seventy-eight days.[17]

Counterinsurgency conflicts, such as those in Afghanistan and Iraq, also necessitate precision military operations that go beyond destroying the enemy's fielded forces.[18] Modern counterinsurgency operations aim to safeguard the State's government, infrastructure and civilian population,

---

13. U.S. CENTRAL COMMAND AIR FORCES, OPERATION IRAQI FREEDOM: BY THE NUMBERS 11 (2003).

14. U.S. Air Force, Factsheet on Joint Direct Attack Munition, GBU-31/32/38, http://www.af.mil/information/factsheets/factsheet.asp?id=108.

15. *Id.*

16. *See* Press Release, North Atlantic Treaty Organization, The Situation In and Around Kosovo: Statement Issued at the Extraordinary Ministerial Meeting of the North Atlantic Council (Apr. 12, 1999), http://www.nato.int/docu/pr/1999/p99-051e.htm.

17. DEPARTMENT OF DEFENSE, KOSOVO/OPERATION ALLIED FORCE AFTER-ACTION REPORT xvii (2000).

18. *See generally* HEADQUARTERS, DEPARTMENT OF THE ARMY & HEADQUARTERS, MARINE CORPS COMBAT DEVELOPMENT COMMAND, FM 3-24/MCWP 3-33.5, COUNTERINSURGENCY (2006).

while waging war against a discrete group within that State.[19] As a result, counterinsurgency air operations emphasize limiting collateral damage, especially civilian casualties, usually at a level far below law of armed conflict requirements. Moreover, airstrikes often target particular insurgents within a group's command and control structure in order to weaken that group's ability to operate cohesively. Since these insurgents often operate among the civilian population, their targeting is operationally challenging and usually only accomplishable through air operations when advanced precision capabilities are available.

Looking toward the future, precision airstrikes will play an ever-increasing role in warfare. Beyond their military utility in terms of finding, fixing, and destroying enemy forces, airstrikes also reduce the risk to the attacker's forces. New weapon systems such as unmanned aerial vehicles, air-based cyber-attack platforms and autonomous systems will further those goals. Of course, as precision attack takes center stage in twenty-first-century warfare, so too will issues as to the law of armed conflict that governs such operations.

III. THE LAW OF ARMED CONFLICT GOVERNING PRECISION AIRSTRIKES

The development of precision airstrike capabilities occurred as the law of armed conflict governing the conduct of hostilities, especially the protection of civilians and civilian objects, began to achieve maturity. Of particular note is the 1977 Protocol Additional I to the 1949 Geneva Conventions, which represented the first codification of such key principles and rules as distinction, proportionality, and precautions in attack.[20] Although the Protocol does not encompass all aspects of air warfare, it expressly applies to "attacks from . . . the air against objectives on land."[21] Among States possessing robust precision attack capabilities, the United States and Israel stand out as non-parties to the treaty. However, both States recognize the

19. *Id.* at 5-1 ("Successful counterinsurgents support or develop local institutions with legitimacy and the ability to provide basic services, economic opportunity, public order, and security. The political issues at stake are often rooted in culture, ideology, societal tensions, and injustice. As such, they defy nonviolent solutions.").

20. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts arts. 48, 51 and 57, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter Additional Protocol I].

21. *Id.*, art. 49(3).

core targeting principles and rules set forth therein as generally reflective of customary international law.[22]

In 2010, a major multiyear research effort sponsored by Harvard University's Program on Humanitarian Policy and Conflict Research and led by Professor Yoram Dinstein produced the *Manual on International Law Applicable to Air and Missile Warfare* (*AMW Manual*).[23] The work, authored by a group of distinguished international law experts and practitioners, represents an unofficial, yet authoritative, restatement of the principles and rules governing aerial operations. In its examination of the key legal issues surrounding precision aerial warfare, this article relies heavily on both the *AMW Manual* and Additional Protocol I as key repositories of the applicable law.

A. Prohibited Weapon Systems

Certain weapon systems and individual weapons are prohibited in aerial warfare irrespective of how they are used or the results their use generates. First, only military aircraft may be used to conduct airstrikes; airstrikes by civilian aircraft are unlawful regardless of how precise they might be.[24] Second, the law of armed conflict forbids the employment of particular weapons on military aircraft even when they are capable of striking a lawful target with great precision and without risk to civilians and civilian objects. These include the following:

> (a) Biological, including bacteriological, weapons[;]
> (b) Chemical weapons[;]
> (c) Laser weapons specifically designed, as their sole combat function or as one of their combat functions, to cause permanent blindness to unenhanced vision, that is to the naked eye or to the eye with corrective eyesight devices[;]

---

22. *See, e.g.,* U.S. Navy, U.S. Marine Corps & U.S. Marine Corps, NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7A, The Commander's Handbook on the Law of Naval Operations ch. 8 (2007) (reiterating most of the Additional Protocol I targeting rules).

23. PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE (2009) [hereinafter AMW MANUAL]. Professor Schmitt served as one of the members of the drafting team for the manual.

24. *Id.*, rule 17(a) ("Only military aircraft, including UCAVs, are entitled to engage in attacks.").

(d) Poison, poisoned substances and poisoned weapons[;]
(e) Small arms projectiles calculated, or of a nature, to cause explosion on impact with or within the human body[; and]
(f) Weapons the primary effect of which is to injure by fragments which in the human body escape detection by x-ray.[25]

B. The Principle of Distinction

The principle of distinction was set forth as early as the 1868 St. Petersburg Declaration,[26] adopted in the 1899 and 1907 Hague Regulations,[27] and codified in Article 48 of Additional Protocol I. The International Court of Justice has described it as one of the two "cardinal" principles of the law of armed conflict.[28] The International Committee of the Red Cross has labeled it the "foundation on which the codification of the laws and customs of war rests."[29]

By the principle, parties to a conflict must distinguish between combatants and military objectives on the one hand and civilians and civilian objects on the other.[30] Once this distinction has been made, they may only attack those targets that qualify as military objectives, combatants, or civilians directly participating in hostilities.[31] In case of doubt as to the targetability of an individual under the law of armed conflict, an individual must be treated as a civilian immune from attack.[32] Precision lies at the heart of

25. *Id.*, rule 6(a)–(f).

26. Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight pmbl. ¶ 2, Dec. 11, 1868, 138 Consol. T.S. 297 ("That the only legitimate objects which States should endeavor to accomplish during war is to weaken the military forces of the enemy.").

27. Convention [II] with Respect to the Laws and Customs of War on Land, with annex of regulations arts. 22, 29, 32, July 29, 1899, Stat. 1803, 32 Stat. 1803, 1 Bevans 247; Regulations Respecting the Laws and Customs of War on Land, annexed to Convention No. 4 Respecting the Laws and Customs of War on Land art. 22, Oct. 18, 1907, 36 Stat. 2277, 1 Bevans 631.

28. Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 78 (July 8).

29. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949 ¶ 1863 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987) [hereinafter ICRC COMMENTARY].

30. Additional Protocol I, *supra* note 20, art. 48.

31. AMW MANUAL, *supra* note 23, rule 10. *See also* Additional Protocol I, *supra* note 20, arts. 51(2), 51(3) and 52(1).

32. Additional Protocol I, *supra* note 20, art. 50(1); *see also* AMW MANUAL, *supra* note 23, rule 12; PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, COMMEN-

the principle of distinction because, as noted, precision involves more than simply striking a particular point (accuracy); it involves hitting the right target in the right way. Therefore, target identification is of paramount importance for both precision warfare and the principle of distinction.

Military objectives, the first category subject to lawful attack, are those "objects which by their nature, location, purpose or use, make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."[33] This definition has two express criteria. First, the object must make an "effective contribution" to enemy operations. While this criterion by no means requires that the contribution be "significant," the object "must in fact contribute to the enemy's military action."[34] Second, the military advantage gained by targeting the object must be "definite." This requires that the advantage not be "merely potential, speculative or indeterminate."[35] ISR is often a necessary component in determining whether these two criteria have been satisfied. If they are not satisfied, then the operation in question is neither a precision strike nor a lawful attack.

Despite universal acceptance of the textual definition of "military objective" set out above, controversy persists over its parameters. Clearly, "war-fighting" targets qualify, as do those that are "war-supporting," such as factories producing munitions or military equipment. However, the United States has taken the position that the term also encompasses "economic targets of the enemy that indirectly but effectively support and sustain the enemy's war-fighting capability."[36] This definition is not widely accepted, as some expert commentators claim it "goes too far" because it does not require the objective to have a "proximate nexus to military action."[37]

TARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE rule 12(a) cmts. 3 and 4 (2010) [hereinafter AMW MANUAL COMMENTARY].

33. AMW MANUAL, *supra* note 23, rule 1(y). This definition is based on Additional Protocol I, *supra* note 20, art. 52(2).

34. AMW MANUAL COMMENTARY, *supra* note 32, rule 1(y) cmt. 4.

35. *Id.*, rule 1(y) cmt. 7. *See also* ICRC COMMENTARY, *supra* note 29, ¶ 2024.

36. ANNOTATED SUPPLEMENT TO THE COMMANDER'S HANDBOOK ON THE LAW OF NAVAL OPERATIONS 402–3 (A. R. Thomas & James C. Duncan eds., 1999) (Vol. 73, U.S. Naval War College International Law Studies) (describing this as a "statement of customary international law").

37. Yoram Dinstein, *Legitimate Military Objectives Under the Current* Jus In Bello, LEGAL AND ETHICAL LESSONS OF NATO'S KOSOVO CAMPAIGN 139, 145–46 (Andru E. Wall ed.,

There are four different ways in which an object may fulfill the two express criteria (i.e., "effective contribution" and "definite military advantage")—through its "nature, location, purpose or use." "Nature" denotes "an inherent characteristic or attribute which contributes to military action."[38] This would include all military equipment and facilities. "Location" relates to "selected areas that have special importance to military operations,"[39] regardless of how those areas are currently being used. A commonly cited example is a mountain pass that, if blocked, would halt an enemy's advance.

"Use" refers to the present function of an object. Those objects that do not qualify as military objectives by "nature" become military objectives by "use" when employed for military purposes, but only for so long as they are so employed. For example, a civilian vehicle may be attacked if enemy forces commandeer it to transport troops, but not once it is returned to its civilian owner.[40] Lastly, "purpose" focuses on the future use of an object. It recognizes that "an attacker need not wait until an object is actually used for military ends before being allowed to attack it as a military objective."[41] Since "purpose" depends on the attacker's perception of the enemy's intent, and since the enemy's intent is not always clear, the attacker must act reasonably.[42] The ability to observe a potential target to determine whether it qualifies as a military objective on one of these four bases is a critical el-

---

2002) (Vol. 78, U.S. Naval War College International Law Studies). On the other hand, some commentators have argued that the term "military objective" should be interpreted even more broadly. *See, e.g.,* Charles J. Dunlap Jr., *The End of Innocence: Rethinking Noncombatancy in the Post-Kosovo Era*, STRATEGIC REVIEW, Summer 2000, at 9, 14); Jeanne M. Meyer, *Tearing Down the Façade: A Critical Look at the Current Law on Targeting the Will of the Enemy and Air Force Doctrine*, 51 AIR FORCE LAW REVIEW 143 (2001).

38. AMW MANUAL COMMENTARY, *supra* note 32, rule 22(a) cmt. 1; *see also* ICRC COMMENTARY, *supra* note 29, ¶ 2020.

39. AMW MANUAL COMMENTARY, *supra* note 32, rule 22(b) cmt; *see also* ICRC COMMENTARY, *supra* note 29, ¶ 2021.

40. AMW MANUAL COMMENTARY, *supra* note 32, rule 22(d) cmt. 1; *see also* ICRC COMMENTARY, *supra* note 29, ¶ 2022.

41. AMW MANUAL COMMENTARY, *supra* note 32, rule 22(c) cmt. 1; ICRC COMMENTARY, *supra* note 29, ¶ 2022.

42. AMW MANUAL COMMENTARY, *supra* note 32, rule 22(c) cmt. 3 ("The attacker must always act reasonably, i.e. as would be proper under a similar set of circumstances for any other Belligerent Party. In other words, the attacker must ask itself whether it would be reasonable to conclude that the intelligence was reliable enough to conduct the attack in light of the circumstances ruling at the time.").

ement of target identification that is often made possible by advanced precision capabilities, most notably ISR.

Like military objectives, combatants are lawful targets and, as with the former, precision capabilities are often a key to their proper identification. Combatants are "[m]embers of the armed forces of a Party to the conflict as well as members of militias or volunteer corps forming part of such armed forces,"[43] excluding "medical or religious personnel."[44] Members of other militias or volunteer corps are also combatants when they fulfill the following cumulative conditions:

(a) Are commanded by a person responsible for his subordinates;
(b) Have a fixed distinctive sign recognizable at a distance;
(c) Carry their arms openly; and
(d) Conduct their operations in accordance with the laws and customs of war.[45]

Note that the term "combatant" is used to describe only participants in an international armed conflict (i.e., a conflict between States). However, "like members of the regular armed forces of the State concerned, members of a non-State organized armed group in a non-international armed conflict are lawful targets."[46]

Civilians directly participating in hostilities may also be targeted.[47] This norm was the subject of a five-year International Committee of the Red Cross project that led to the 2009 publication of the *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*.[48] Of particular importance is the *Guidance*'s delineation of the consti-

43. Convention Relative to the Treatment of Prisoners of War art. 4, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 [hereinafter Geneva Convention III]; *see also* AMW MANUAL COMMENTARY, *supra* note 32, rule 10(b)(i) cmt. 1.

44. AMW MANUAL COMMENTARY, *supra* note 32, rule 10(b)(i) cmt. 2.

45. Geneva Convention III, *supra* note 43, art. 4(A)(2). *See also* AMW MANUAL COMMENTARY, *supra* note 32, rule 10(b)(i) cmt. 2.

46. AMW MANUAL COMMENTARY, *supra* note 32, rule 10(b); *see also* NILS MELZER, INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION IN HOSTILITIES UNDER INTERNATIONAL HUMANITARIAN LAW 36 (2009) [hereinafter ICRC INTERPRETIVE GUIDANCE].

47. Additional Protocol I, *supra* note 20, art. 51(3); *see also* Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts art. 13(1), June 8, 1977, 1125 U.N.T.S. 609; AMW MANUAL, *supra* note 23, rule 28.

48. ICRC INTERPRETIVE GUIDANCE, *supra* note 46.

tutive elements of direct participation. By that standard, an act qualifying an individual as a direct participant "must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack."[49] There must also be a causal connection between the act and the harm and the act must exhibit belligerent nexus.[50] Controversy remains over both the precise criteria for determining that a civilian is directly participating in hostilities[51] and as to when the direct participant may be lawfully attacked.[52] Despite these debates, the premise that civilians directly participating in hostilities may be targeted is widely accepted, and precision technology is invaluable in determining whether a civilian is participating as such.

C. Prohibition against Indiscriminate Attack

The law of armed conflict prohibits indiscriminate attacks, which are "those that cannot be or are not directed against lawful targets . . . or the effects of which cannot be limited as required by the law of international armed conflict, and which therefore are of a nature to strike lawful targets and civilians or civilian objects without distinction."[53] In other words, the

---

49. *Id.* at 47.

50. *Id.* at 46–64.

51. AMW MANUAL COMMENTARY, *supra* note 32, rule 29 cmt. 5.

52. *Id.*, rule 28 cmt. 3. For a more robust examination of the various points of contention, see, e.g., Kenneth Watkin, *Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 641 (2010); Michael N. Schmitt, *Deconstructing Direct Participation in Hostilities: The Constitutive Elements*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 697 (2010); Bill Boothby, *"And for Such Time As": The Time Dimension to Direct Participation in Hostilities*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 741 (2010); W. Hays Parks, *Part IX of the ICRC "Direct Participation in Hostilities" Study: No Mandate, No Expertise, and Legally Incorrect*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 769 (2010); Nils Melzer, *Keeping the Balance between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS (2010).

53. AMW MANUAL, *supra* note 23, rule 13 (b); *See also* Additional Protocol I, *supra* note 20, art. 54. For the prohibition on indiscriminate attack as part of customary international law, see, e.g., Prosecutor v. Martic, Case No. IT-95-11-T, Judgment, ¶ 463 (Int'l Crim. Trib. for the former Yugoslavia June 12, 2007) (holding that firing high-dispersion non-guided rockets at a densely populated civilian area constituted an indiscriminate attack).

notion of indiscriminate attack encompasses both the use of weapons incapable of discriminating between lawful and unlawful targets and the use of weapons that, albeit capable of being directed at a lawful target, are used indiscriminately. Indiscriminate attacks are the antithesis of precision warfare.

A violation of the prohibition against indiscriminate use of a lawful weapon typically involves reckless disregard for the safety of civilian persons or objects.[54] At its most basic level, an indiscriminate attack is one where the weapon system could be aimed, but the attacker fails to do so, as in the case of blindly dropping bombs over enemy territory. Other examples include an attack based on patently unreliable information and one in which the weapon is employed in an environment that causes it to be highly inaccurate (e.g., at a very high altitude or in weather that disrupts guidance system functionality). As these examples demonstrate, every aspect of a precision airstrike (accuracy, C4ISR and outside factors) can prove determinative as to whether a strike is indiscriminate as a matter of law.

The prohibition also extends to certain types of "target area" bombing since "[a]ttacks must not treat as a single lawful target a number of clearly separated and distinct lawful targets located in a city, town, village or area containing a similar concentration of civilians or civilian objects."[55] Compliance with this norm is directly related to the precision capabilities of the weapon systems involved. If those capabilities afford an attacker the option of individually attacking lawful targets in the area, it must do so. On the other hand, if the systems used are insufficiently precise to mount separate attacks, the area itself may be attacked (so long as the attack comports with the rule of proportionality and the requirement to take precautions in attack).

Use of indiscriminate weapons is likewise prohibited.[56] As noted above, certain weapons are prohibited per se from use, often because of their indiscriminate character.[57] All other weapons are analyzed on a case-by-case basis.[58] They may be proscribed as indiscriminate on two grounds.

---

54. YORAM DINSTEIN, THE CONDUCT OF HOSTILITIES UNDER THE LAW OF INTERNATIONAL ARMED CONFLICT 126–28 (2010).

55. AMW MANUAL, *supra* note 23, rule 13(c); *see also* Additional Protocol I, *supra* note 20, art. 51(5).

56. The International Court of Justice has labeled the prohibition on indiscriminate weapons "cardinal." Nuclear Weapons Advisory Opinion, *supra* note 28, ¶ 105E.

57. *See* AMW MANUAL COMMENTARY, *supra* note 32, rule 6.

58. *See id.*, rule 13(a) cmt. 2.

First, weapons cannot be used if they are incapable of being reliably aimed at a military objective. The paradigmatic example is the German V-2 rocket employed during World War II. Its guidance system was such that any attempt to use it to attack a particular military objective within its range, including large objectives such as military installations, would likely fail; a successful attack would effectively be the product of luck. The precision capabilities of most contemporary weapon systems would preclude them from running afoul of this prohibition. For instance, even in the case of unguided (gravity or "dumb") bombs, delivery methodologies have been developed which provide the weapon system (aircraft and bomb) a degree of accuracy.

Second, the use of weapons that have uncontrollable effects is unlawful. The most commonly cited examples are biological contagions or persistent airborne chemicals that, even if accurately aimed at enemy forces, could easily spread to the civilian population. Both are by nature indiscriminate, a fact that explains their long-standing prohibition.[59]

International law's application and understanding of the rules prohibiting indiscriminate attacks will evolve with advances in precision weaponry. For example, while bombs dropped from a B-17 during World War II had a circular error probable exceeding three thousand feet, today such accuracy (or lack thereof) would be considered indiscriminate. In the future, it is plausible that unguided air-delivered weapons as such may begin to be characterized as violating the prohibition.

D. Proportionality

The rule of proportionality prohibits an "attack that may be expected to cause collateral damage which would be excessive in relation to the concrete and direct military advantage anticipated."[60] It applies when an attack is properly directed at a lawful target but "collateral damage" is neverthe-

59. *See* AMW MANUAL, *supra* note 23, rule 6; Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 26 U.S.T. 571; Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, Jan. 13, 1993, 1974 U.N.T.S. 45; Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction, Apr. 10, 1972, 1015 U.N.T.S. 163.

60. AMW MANUAL, *supra* note 23, rule 14; *see also* Additional Protocol I, *supra* note 20, arts. 51(5)(b) and 57(2)(b). For proportionality as part of customary law of armed conflict, see Nuclear Weapons Advisory Opinion, *supra* note 28, ¶ 105E (Higgins, J., dissenting).

less unavoidable. Collateral damage consists of "incidental loss of civilian life, injury to civilians and damage to civilian objects or other protected objects or a combination thereof, caused by an attack on a lawful target."[61] Recognized injuries do not include mere inconvenience or fear among the civilian population.[62] While there is some dispute regarding the extent to which "indirect effects" of an airstrike must be taken into account when assessing proportionality, general agreement exists that consequences should not be included in the proportionality analysis if they are "too remote or cannot be reasonably foreseen."[63]

Military advantage, the factor in the context of which collateral damage is considered, consists of "those benefits of a military nature that result from attack."[64] Although certain commentators argue that the term includes only "ground gained" and "annihilating or weakening the enemy armed forces,"[65] the *AMW Manual* suggests the "better approach" is to include "any consequence of an attack which directly enhances friendly military operations or hinders those of the enemy."[66] Consider a precision airstrike that does not destroy an enemy armored column, but instead reduces its mobility by, for example, destroying a bridge across which it would pass. The *AMW Manual* would properly characterize the diminished mobility of the column as a military advantage.

Key to correct application of the proportionality analysis is an emphasis on what is "expected" and "anticipated." When performing a proportionality analysis, an attacker has to anticipate the likely consequences of a strike; the focus is on expectations, not results. These expectations must be "reasonable" in the sense that a "good faith assessment by the commander planning or approving the attack" would conclude that the outcome is "probable, i.e. more likely than not."[67] The reasonableness requirement attaches at every stage of an attack. Accordingly, an individual with the authority or ability to suspend an attack must do so if, at any point, he or she concludes that an operation would cause excessive collateral damage in re-

---

61. AMW MANUAL, *supra* note 23, rule 1 (l); *see also* Additional Protocol I, *supra* note 20, art. 51(5).

62. AMW MANUAL COMMENTARY, *supra* note 32, rule 1(l) cmt 5.

63. *Id.*, rule 14 cmt. 4.

64. AMW MANUAL, *supra* note 23, rule 1(w).

65. ICRC COMMENTARY, *supra* note 29, ¶ 2218.

66. AMW MANUAL COMMENTARY, *supra* note 32, rule 1(w) cmt. 3.

67. *Id.*, rule 14 cmt. 6. Similarly, proportionality requires that the military advantage be "concrete and direct," meaning it must be "clearly identifiable" instead of "based merely on hope or speculation." *Id.*, rule 14 cmt. 9.

lation to the anticipated military advantage.[68] Both the commander who approves a mission and the aircrew that flies it would, for example, be included.

Precision is highly determinative of both the collateral damage and the military advantage that are likely to result from a strike. Attackers must consider such factors as the timeliness, reliability and comprehensiveness of target intelligence, the accuracy of the weapon system, and the effect of environmental factors when forming their expectations or anticipations.

Once the collateral damage and military advantage are estimated, the attacker has to determine whether the former is "excessive" relative to the latter. While the *AMW Manual* defines "excessive" as a "significant imbalance,"[69] it must be remembered that proportionality does not involve a strict mathematic balancing test. Such a test would be conceptually and practically impossible in that it would require commanders and others performing a proportionality analysis to value and compare dissimilar entities. For example, how is an attacker supposed to estimate how much a tank is "worth" in terms of civilian deaths or civilian property damage? The excessiveness standard avoids the legal fiction that the value of these dissimilar entities can be quantified along a single axis. Instead, it bans attacks in which proportionality between the ends sought and the expected harm to civilians and civilian objects is absent altogether. Restated, the test is simply one of reasonableness in the prevailing circumstances.

Since excessiveness is determined only in relation to the military advantage an attacker reasonably anticipates gaining, as the potential military advantage estimate grows so does the acceptable extent of likely collateral damage. While some have asserted that any attack resulting in "extensive" collateral damage is forbidden,[70] this is wrong as a matter of law; there is no absolute threshold of collateral damage above which the rule of proportionality ceases to apply and an attack is prohibited.[71] Instead, proportionality assessments must be made for every attack and they are always contextual.[72] Depending on the military advantage anticipated to result, some

68. *Id.*, rule 14 cmt. 15; *see also* Additional Protocol I, *supra* note 20, art. 57(2)(b).

69. AMW MANUAL COMMENTARY, *supra* note 32, rule 14 cmt. 7.

70. ICRC COMMENTARY, *supra* note 29, ¶ 1980.

71. AMW MANUAL COMMENTARY, *supra* note 32, rule 14 cmt. 8.

72. *See, e.g.,* Nuclear Weapons Advisory Opinion, *supra* note 28, ¶ 105E (holding that the Court could not "conclude definitively whether the threat or use of nuclear weapons would be lawful or unlawful in an extreme circumstance of self-defence, in which the very survival of a State would be at stake").

highly precise strikes may cause collateral damage that qualifies as excessive, while attacks employing no precision systems may sometimes result in collateral damage that is not excessive in light of the military gain sought.

Improvements in precision airstrike capabilities will unquestionably exercise a direct influence on how proportionality will be understood in future combat operations. As noted in the context of indiscriminate attacks, standards generally become more restrictive with advances in precision technology. Therefore, as the capacity to conduct precision airstrikes grows, attitudes toward the acceptability of collateral damage under the law of armed conflict (i.e., what is considered "excessive") will likely become more demanding.

E. Precautions in Attack

The law of armed conflict requires that "[c]onstant care must be taken to spare the civilian population, civilians and civilian objects."[73] "Constant care" entails taking certain "feasible precautions" both before and during a strike.[74] The precautions are designed to ensure, to the extent possible, that only lawful targets are attacked and collateral damage is minimized. The availability of precision capabilities affects compliance with most of the obligatory precautionary measures.

Article 57 of Additional Protocol I generally codifies the specific precautions, each of which is reflected in the *AMW Manual*. These precautions need only be taken when doing so is "feasible." "Feasible" denotes a measure of precaution that "is practicable or practically possible, taking into account all circumstances prevailing at the time, including humanitarian and military considerations."[75] What is considered practicable or practically possible has been described as "a matter of common sense and good faith."[76]

At its core, feasibility is a reasonableness standard—those who plan, approve or execute an attack have to undertake any measures to limit harm

---

73. AMW MANUAL, *supra* note 23, rule 30. *See also* Additional Protocol I, *supra* note 20, art. 57(1).

74. *See* Additional Protocol I, *supra* note 20, art. 57; AMW MANUAL, *supra* note 23, rules 30–33.

75. AMW MANUAL, *supra* note 23, rule 1(q); *see also* Amended Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices art. 3(10), May 3, 1996, 2048 U.N.T.S. 93.

76. ICRC COMMENTARY, *supra* note 29, ¶ 2198.

to civilians and civilian objects that a reasonable warfighter in the same or similar circumstances would take. Of course, attackers are only required to take into account information that is "reasonably available"[77] to them "at the relevant time and place."[78] Furthermore, in deciding whether a measure is feasible, they may factor in military considerations, such as the availability of precision weapons, competing demands for surveillance capabilities and risk to friendly forces.

As to specific measures, attackers must first do everything feasible to verify that the target is a lawful one and does not benefit from specific protection.[79] Determining which objectives qualify as lawful targets requires an attacker to utilize reasonably available ISR assets to gain information about the target. In particular, the "quality and timeliness of the intelligence has to be considered," including the potential that the "enemy may attempt to provide disinformation."[80] An attacker should also assess the availability of other sources of intelligence, such as "on the spot" visual observations.[81]

The requisite level of certainty as to target identification is not entirely clear. Some commentators appear to require near certainty.[82] However, such a standard would ignore the realities of combat, in which attackers operate in the fog of war. A more manageable standard that comports with the notion of feasibility asks whether a reasonable warfighter, having exhausted all reasonably available means of verification in light of the prevailing circumstances, would launch the attack. This standard allows attackers to balance the potential military advantage against both the likely collateral damage and any degree of doubt as to the objective's status as a lawful target, just as the law of armed conflict allows military advantage to offset collateral damage more generally. Obviously, precision capabilities play a key role in this process, especially ISR assets that allow targets to be located, monitored and identified. While these capabilities have immense military utility, they can also be constraining. If a "reasonable warfighter in the same or similar circumstances" would consider their use both helpful in

77. AMW MANUAL, *supra* note 23, rule 32(a).

78. AMW MANUAL COMMENTARY, *supra* note 32, rule 1(q) cmt. 3.

79. AMW MANUAL, *supra* note 23, rule 32(a); *see also* Additional Protocol I, *supra* note 20, art. 57(2)(a)(i).

80. *See* AMW MANUAL COMMENTARY, *supra* note 32, rule 32(a). cmt. 2.

81. *Id.*

82. *See, e.g.*, ICRC COMMENTARY, *supra* note 29, ¶ 2195 ("[I]n case of doubt, even if there is only slight doubt, [those who plan or decide upon attack] must call for additional information.").

identifying an objective and feasible, an attack not employing such capabilities would be unlawful.

Similarly, the requirement to take precautions in attack also mandates that an attacker choose from among feasible means (weapons) and methods (tactics) of warfare in order to minimize collateral damage.[83] As with target identification, precision capabilities can act as a double-edged sword when complying with this required precaution. While helpful both militarily and in conforming to the law of armed conflict, precision capabilities can also force an attacker's hand when their use is mandatory under this rule. After all, since precision capabilities usually allow for greater accuracy and lesser explosive force, their use (when available) may be required as a matter of law when the result would be less harm to civilians and civilian property.

This rule has two important caveats. First, States are not required to acquire or field precision capabilities.[84] The battlefield is "come as you are" in the law of armed conflict. Second, even when an attacker has precision capabilities available and their use would limit civilian harm, employment is compulsory only when feasible.[85] For example, precision capabilities may be in short supply at the time of attack. In such a situation, a commander may preserve some or all of his or her precision weapons for later operations, taking into account both military and humanitarian concerns. The paradigmatic example is retention for use in impending urban operations, where precision weapons will prove highly useful in avoiding collateral damage.

A third key precaution in attack applies when an attacker has a choice between several military objectives the destruction of which would result in

---

83. AMW MANUAL, *supra* note 23, rule 32 (b); *see also* Additional Protocol I, *supra* note 20, art. 57(2)(a)(ii).

84. AMW MANUAL, *supra* note 23, rule 8. *See also* DINSTEIN, *supra* note 54, at 142 ("No [law of international armed conflict] LOIAC obligation is incumbent on Belligerent Parties to use expensive 'smart bombs' where cheaper 'dumb bombs' will do.").

85. AMW MANUAL, *supra* note 23, rules 31–32. However, some claim there is a duty to use precision munitions whenever available or at least in certain environments (e.g., urban areas). *See, e.g.,* Stuart W. Belt., *Missiles over Kosovo: Emergence,* Lex Lata*, of a Customary Norm Requiring Use of Precision Munitions in Urban Areas*, 47 NAVAL LAW REVIEW 115, 174 (2000); Danielle L. Infeld, *Precision-Guided Munitions Demonstrated Their Pinpoint Accuracy in Desert Storm; But Is a Country Obligated to Use Precision Technology to Minimize Collateral Civilian Injury and Damage?*, 26 GEORGE WASHINGTON UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND ECONOMICS 109, 110–11 (1992). Both assertions are wrong as the decision is always fully contextual.

a similar military advantage. In that situation, an attacker must select the objective which, when attacked, would involve the least danger to civilian lives and civilian objects or to other protected persons and objects.[86] Here again, precision capabilities may have a restrictive effect on an attacker to the extent that they increase the number of potential targets that can be feasibly attacked. As with the other precautions though, the only objectives that need be considered are those on which an attack is militarily reasonable. For example, imagine there are two potential targets the destruction of which would yield the same military advantage. One is heavily defended, but remote from civilians, while the other has few defenses, but is located in the vicinity of civilians and civilian structures. In this situation, the targeting of the heavily defended objective would not be required, even though its destruction would offer a "similar military advantage" and cause less collateral damage.[87]

IV. LOOKING FORWARD: A NEW GENERATION OF PRECISION WEAPON SYSTEMS

Three relatively new weapon systems—unmanned combat aerial vehicles (UCAV), autonomous weapon systems, and cyber-attack systems—have captured the attention of the law of armed conflict community. Each raises issues of precision that merit careful reflection.

A. Unmanned Combat Aerial Vehicles

An unmanned combat aerial vehicle, commonly referred to as a "drone," is an "unmanned military aircraft of any size which carries and launches a weapon, or which can use on-board technology to direct such a weapon to a target."[88] The use of UCAVs has dramatically grown over the past dec-

86. AMW MANUAL, *supra* note 23, rule 33; *see also* Additional Protocol I, *supra* note 20, art. 57(3).

87. However, the risk to military personnel must still be balanced against the risk of collateral damage. AMW MANUAL COMMENTARY, *supra* note 32, rule 1(q) cmt. 5 ("[W]hereas a particular course of action may be considered non-feasible due to military considerations (such as excessive risks to aircraft and their crews), some risks have to be accepted in light of humanitarian considerations.").

88. AMW MANUAL, *supra* note 23, rule 1(ee). Within the U.S. Air Force unmanned aerial vehicles are commonly referred to as "remotely piloted aircraft" (RPA). U.S. Air Force, AFDD 1-02, Air Force Supplement to the Department of Defense Dictionary of

ade, a trend which is certain to continue.[89] This is understandable in light of their ability to employ precision weapons using enhanced ISR capabilities in an operation that poses no risk to the aircrew conducting the mission.

While the law of armed conflict principles and rules discussed in Part III apply with equal force to UCAV operations,[90] the unique precision capabilities UCAVs offer commanders influence their application, especially with regard to the requirement to take precautions in attack. The fact that a UCAV sortie poses no risk to the aircrew enhances the feasibility of their use in high-threat environments, thereby increasing the precision of the strike itself and making possible attacks on alternative targets that might not otherwise be viable. Onboard ISR capabilities, such as sensors and cameras, and the ability of UCAVs to loiter over a target for extended periods, bolster their ability to identify a target. UCAV ISR capabilities also minimize the likelihood, or degree, of collateral damage by making possible execution of the attack when civilians and civilian objects are least likely to be harmed. Additionally, UCAVs are armed only with precision weaponry, thereby providing commanders an effective option when selecting methods and means of warfare with the goal of minimizing civilian harm in mind.

B. Automated Weapon Systems

Developments in automated weapons technology have led some States to "envision a world in which humans need not be in the decision loop."[91]

Military and Associated Terms (Jan. 11, 2007, incorporating Change 1, Jan 6. 2012), *available at* https://www.fas.org/irp/doddir/usaf/afdd1-2.pdf.

89. For example, the Department of Defense is dramatically increasing reliance on UCAVs and other drones. Adam Entous et al., *More Drones, Fewer Troops*, WALL STREET JOURNAL, Jan. 27, 2012, at 10.

90. *See, e.g.,* Michael N. Schmitt, *Unmanned Combat Aircraft Systems (Armed Drones) and International Humanitarian Law: Simplifying the Oft Benighted Debate,* 30 BOSTON UNIVERSITY INTERNATIONAL LAW JOURNAL 595, 609 (2012); Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, *Study on Targeted Killings* ¶ 79, Human Rights Council, U.N. Doc. A/HRC/14/24/Add.6 (May 28, 2010) (by Philip Alston), *available at* http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf ("[A] missile fired from a drone is no different from any other commonly used weapon, including a gun fired by a soldier or a helicopter or gunship that fires missiles. The critical legal question is the same for each weapon: whether its specific use complies with [international humanitarian law].").

91. U.S. JOINT FORCES COMMAND, UNMANNED EFFECTS (UFX): TAKING THE HUMAN OUT OF THE LOOP 4 (2003). *See also* U.S. AIR FORCE, UNMANNED AIRCRAFT SYSTEMS FLIGHT PLAN 2009-2047, at 41 (2009).

Such "fully autonomous weapon systems" would be capable of identifying potential targets, selecting them for attack and striking them without human interface.[92] Armed forces around the world are extremely interested in these systems since the operation of manned weapon systems can be personnel intensive and dangerous, while systems that are operated remotely, such as UCAVs, are vulnerable to communications jamming or cyber attack.

Fully autonomous weapon systems must be distinguished from other systems. For example, "human-supervised" autonomous systems—such as Israel's Iron Dome—have been in operation for years.[93] These systems have a "human in the loop" that closely monitors an engagement and can override the system if needed. Certain other weapon systems such as the "close-in weapon system"[94] can be programmed to operate autonomously, but are presently used solely for point defense in accordance with very narrow fixed parameters.

The fact that autonomous weapon systems have become both militarily desirable and technologically feasible is spawning interest in the legal issues surrounding their use.[95] Indeed, Human Rights Watch has asserted the weapon systems would be "unable to meet legal standards" and therefore

---

92. An autonomous weapons system is defined as:

> a weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.

Deputy Secretary of Defense, DoDD 3000.09, Autonomy in Weapon Systems 13–14 (Nov. 21, 2012).

93. Iron Dome can operate automatically using programmed parameters, but the system also allows for human operator intervention. Inbal Orpaz, *How Does Iron Dome Operate?*, HAARETZ (Nov. 19, 2012), http://www.haaretz.com/news/features/how-does-the-iron-dome-work.premium-1.478988.

94. *See generally* U.S. Navy, *MK 15—Phalanx Close-In Weapons System (CIWS)*, http://www.navy.mil/navydata/fact_display.asp?cid=2100&tid=487&ct=2.

95. *See generally* Michael N. Schmitt & Jeffrey S. Thurnher, "*Out of the Loop": Autonomous Weapon Systems and the Law of Armed Conflict*, 4 HARVARD NATIONAL SECURITY JOURNAL 231 (2013); Kenneth Anderson & Matthew Waxman, *Law and Ethics for Robot Soldiers*, 176 POLICY REVIEW (Dec. 1, 2012), http://www.hoover.org/publications/policy-review/article/135336; Markus Wagner, *Taking Humans Out of the Loop: Implications for International Humanitarian Law*, 21 JOURNAL OF INFORMATION AND SCIENCE 155 (2011).

"should be banned."[96] Pronouncements of illegality are premature at best and more likely simply wrong. As with most weapon systems, the principal normative issues involve use of the systems, not their possible status as unlawful weapons per se. Unsurprisingly, most of the challenging legal questions bear on the degree of precision the systems might be able to achieve.

For example, Human Rights Watch contends that autonomous weapons violate the prohibition on indiscriminate attacks because "[f]ully autonomous weapon systems would not have the ability to sense or interpret the difference between soldiers and civilians, especially in contemporary combat environments."[97] There are two problems with this statement. First, it ignores the fact that some battlespaces contain no civilian persons or objects. In such environments, fully autonomous systems that are unable to identify civilian persons or objects could still be used without violating the prohibition on indiscriminate attacks because there is no chance of harming civilian persons or objects. Second, and perhaps more importantly, the statement assumes that no technological developments will afford fully autonomous systems an ability to distinguish between military and civilian personnel and objects.[98] This is a curious stance since the ability of weapon systems to discriminate on the battlefield has been growing exponentially due to technological advances, often in ways that seemed unimaginable only a few years earlier.

The ability of autonomous weapon systems to comply with the principle of proportionality has likewise been questioned.[99] If there is no "human in the loop," the weapon system would have to both estimate the likely collateral damage and determine whether that damage is excessive relative to

---

96. HUMAN RIGHTS WATCH, LOSING HUMANITY: THE CASE AGAINST KILLER ROBOTS 1–2 (2012), *available at* http://www.hrw.org/reports/2012/11/19/losing-humanity-0.

97. *Id.* at 30.

98. The current state of technology already allows computers to recognize many things:

> Modern sensors can, *inter alia*, assess the shape and size of objects, determine their speed, identify the type of propulsion being used, determine the material of which they are made, listen to the object and its environs, and intercept associated communications or other electronic emissions. They can also collect additional data on other objects or individuals in the area and, depending on the platform with which they are affiliated, monitor a potential target for extended periods in order to gather information that will enhance the reliability of identification and facilitate target engagement when the risk of collateral damage is low.

Schmitt & Thurnher, *supra* note 95, at 297.

99. HUMAN RIGHTS WATCH, *supra* note 96, at 32.

the military advantage anticipated to result from the attack. While critics rightly suggest that current technology is incapable of performing this task, future autonomous weapon systems will likely be programmable to perform analysis similar to the collateral damage estimate methodology (CDEM)[100] currently used to determine the likelihood of harm to civilians or civilian objects in a target area. After all, CDEM relies on objective data and scientific algorithms. The resulting collateral damage estimate could then be used as the basis for "proportionality red lines" which, given the type of target being engaged, would preclude attack based on pre-programmed criteria.

The potential use of these weapons raises difficult legal questions. However, until the degree of precision they can achieve becomes clearer, any ban on their use would be rash. Indeed, it is conceivable that future fully autonomous systems might be more precise and better able to distinguish lawful targets from civilians and civilian objects than their manned or remotely operated counterparts.

C. Cyber Attacks

Cyber attacks launched from or through airborne platforms are by their very nature accurate. As with more traditional precision airstrikes, cyber attacks will almost always involve extensive C4ISR capabilities. Not only are advanced computer and communications capabilities required to mount these attacks, but increased cyber security has made cyber intelligence, surveillance and reconnaissance essential because the potential vulnerabilities of any target system must be identified and understood before effective exploitation is possible. Furthermore, attacking those vulnerabilities may require computer code specifically designed to exploit a particular vulnerability.

The law of armed conflict principles and rules discussed in Part III apply only to those cyber operations that qualify as an "attack."[101] As a term of art in the law of armed conflict, an attack is defined as "an act of vio-

100. For a discussion of the methodology, see Defense Intelligence Agency General Counsel, Briefing: Joint Targeting Cycle and Collateral Damage Estimate Methodology (CDM), Nov. 10, 2009, http://www.aclu.org/files/dronefoia/dod/drone_dod_ACLU_DRONES_JOINT_STAFF_SLIDES_1-47.pdf.

101. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE, ch. 4, § 2, cmts. 1–3 (Michael N. Schmitt ed., 2013) [hereinafter TALLINN MANUAL].

lence, whether in offence or in defence."[102] This includes non-kinetic operations, such as computer operations that "result in death, injury, damage or destruction of persons or objects."[103]

In the absence of State practice, all predictions as to how the law of armed conflict will eventually shape the use of cyber attacks remain highly speculative. That said, it is probable that the extant law will, as it has with other new weapon systems, generally suffice to govern cyber-weapon systems, albeit with some interpretive accommodation for the unique characteristics of cyberspace. In particular, the interconnectivity of military and civilian cyber systems may result in a greater demand for precision than is the case with kinetic weaponry. For instance, the prohibition on indiscriminate attacks could in the future be interpreted to restrict the use of certain malware against military objectives that rely on dual-use (civilian/military) networks. Similarly, the precautions in attack rules may be interpreted to require a certain degree of target network mapping due to the risk of bleed-over into civilian systems.

Due to the immense non-physical damage that cyber operations are capable of causing, it is also possible that, over time, the law of armed conflict will evolve in response. For example, it is conceivable that the current understanding of what constitutes an attack may expand to include certain cyber operations that do not cause physical injury or damage, thereby prohibiting the directing of such operations at protected persons and objects. This sort of shift in understanding may similarly end up expanding what qualifies as collateral damage. Beyond any evolution in the application of current law of armed conflict principles, new prohibitions may also be adopted that provide special protection for certain civilian objects, such as critical infrastructure. Any of these potential changes—lowering the threshold for what constitutes an attack, expanding the definition of collateral damage or adopting a new group of protected objects—would require heightened precision capabilities.

---

102. AMW MANUAL, *supra* note 23, rule 1(e). Additional Protocol I, *supra* note 20, art. 49.

103. AMW MANUAL COMMENTARY, *supra* note 32, rule 1(e) cmt. 7. *See also* TALLINN MANUAL, *supra* note 101, rule 30 ("[A] cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.").

V. CONCLUSION

Precision lies at the heart of both contemporary air warfare and the law of armed conflict rules that govern it. Precision capabilities increase an attacker's ability to distinguish between military and civilian objectives, thereby fostering compliance with the principle of distinction. Furthermore, the accuracy and C4ISR capabilities that are integral to precision weaponry mean that such weapons cannot be deemed indiscriminate. On the contrary, the increased ability to gather information about a target, distinguish lawful from unlawful targets and strike lawful targets with great accuracy help to ensure that attacks are neither indiscriminate nor violative of the principle of proportionality. Additionally, precision capabilities expand the means, methods and target options that are available to an attacker. This increases an attacker's feasible options in planning and executing airstrikes, thereby increasing the influence of the precautions in attack rules on air operations.

This does not mean that precision capabilities are a panacea. Of course, precision capabilities may be used in an unlawful manner. Perhaps most nefariously, precision can facilitate surgical strikes against protected persons or places such as religious or political leaders, gatherings of particular ethnic groups or cultural property. But in general, precision capabilities contribute positively to humanitarian ends.

While precision capabilities make possible attacks that the law of armed conflict would otherwise prohibit by limiting the risk of harm to civilians and civilian objects, such capabilities also act as a restraint on air operations in some situations. In particular, the requirements of precautions in attack may either mandate the use of precision capabilities before an attack is launched or prohibit an attack on an otherwise lawful target when another option is available that poses less risk to civilians or civilian objects. This is so even when the enemy may not be restricted in this manner, because it lacks precision systems. In other words, the law is relative; one side's precision capabilities may prohibit it from conducting operations open to its enemy.

In the future, demands for precision will unquestionably intensify. The expectations of the global community as to precision capabilities have grown steadily since the Vietnam conflict and show no sign of abating. On the contrary, the counterinsurgency campaigns in Iraq and Afghanistan heightened expectations because they were so restrictive in terms of collateral damage. The fact that operational and policy concerns, not legal con-

straints, drove the restrictions has gone unnoticed by many. Additionally, the advent of unmanned and cyber systems, both of which offer precision capabilities not otherwise available on the battlefield, will further amplify expectations as the international law community begins to grasp their potential to avoid civilian harm. Once this occurs, the interpretation and application of law of armed conflict norms regarding targeting will inexorably evolve, as they always have, with advances in precision technology.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Global Armed Conflict? The Threshold of Extraterritorial Non-International Armed Conflicts

Sasha Radin

89 INT'L L. STUD. 696 (2013)

Volume 89 2013

Global Armed Conflict? The Threshold of Extraterritorial Non-International Armed Conflicts

Sasha Radin[*]

I. INTRODUCTION

On February 4, 2013 the National Broadcasting Corporation (NBC) published a leaked U.S. Department of Justice White Paper outlining the U.S. government's legal authority to kill American citizens who occupy senior operational roles within Al Qaeda.[1] In addition to raising domestic constitutional questions, the White Paper cast renewed attention upon a number of contentious international law issues. These concerns, which all stem from a lack of clarity as to when a State may conduct hostilities against armed groups located outside its borders, include the extent of a State's

* Visiting Research Scholar at the Naval War College, Newport Rhode Island; PhD candidate, Asia Pacific Centre for Military Law, University of Melbourne Law School. For helpful comments and conversations, special thanks to Jann Kleffner, Michael Schmitt, Kinga Tibori-Szabó, Michelle Lesh, Lieutenant Commander James Farrant, Lieutenant Colonel Jeffrey S. Thurnher, Marko Divac Oberg and Captain Ralph Thomas (Ret.).

1. U.S. Department of Justice, *Lawfulness of a Lethal Operation Directed against a U.S. Citizen Who Is a Senior Operational Leader of Al-Qaeda or an Associated Force* (2011), *available at* http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf [hereinafter DOJ White Paper].

right of self-defense against the actions of an armed group in a second State; the question of when the law of armed conflict (LOAC) is triggered; and the body of law that applies to individuals affiliated with an armed group, yet who are located in a second State at a distance from the main area of hostilities. As part of that broader discussion, this article focuses on the question of when hostilities with armed groups operating across State borders may be classified as an armed conflict, and therefore subject to LOAC. The latter issue of what law is applicable to individuals located away from the battlefield once an armed conflict exists is also briefly addressed.

This topic has particular relevance today given the frequency with which armed groups disregard State boundaries in conducting their operations and the ambiguity surrounding the applicable legal framework. The law of armed conflict is structured around State-centric concepts of sovereignty and territory, and is designed for either inter-State conflicts or for purely internal armed conflicts.[2] Its contours have been based on territorial boundaries.[3] Thus, international armed conflicts (IACs)[4] may generally only occur between States.[5] Non-international armed conflicts (NIACs),[6] or

2. For an interesting historical discussion of the territorialized thinking influence upon the development of LOAC, see Louise Arimatsu, *Territory, Boundaries and the Law of Armed Conflict*, 12 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 157 (2009).

3. *Id.* at 170.

4. The main treaties applicable to international armed conflicts are: Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Aug. 12 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 [hereinafter GC III]; Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3 [hereinafter AP I].

5. *See* COMMENTARY TO GENEVA CONVENTION III RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 23 (Jean Pictet ed., 1960) [hereinafter GC III COMMENTARY] ("Any difference arising between two States and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2."); Prosecutor v. Tadić, Case No. IT-94-1-AR72, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the former Yugoslavia Oct. 2, 1995) [hereinafter *Tadić* Appeals Decision on Jurisdiction]. Recognized belligerencies and the controversial Article 1(4) of AP I are exceptions.

6. The law applicable to NIACs is found in Article 3 Common to the Geneva Conventions of 1949 (Common Article 3) and in Protocol Additional to the Geneva Conven-

conflicts where armed groups either fight a State or each other, have traditionally been geographically limited to the confines of a State.[7]

Conflicts such as the Israeli-Hezbollah war of 2006, the ongoing conflict in Afghanistan that has spilled over into Pakistan and the U.S. global armed conflict against Al Qaeda[8] challenge this traditional State-centric structure of LOAC. As a result, there is considerable debate as to how such extraterritorial hostilities (i.e., those that cross State borders) should be characterized. If hostilities do not rise to the level of an armed conflict, they fall under a law enforcement regime[9] and are governed mainly by domestic law and international human rights law. Although extraterritorial hostilities do not fit neatly into any of these three existing legal divisions—IACs, NIACs or law enforcement—their categorization has serious practical implications. Particularly, the classification of conflict affects such matters as how force may be used, what rules apply for detention and whether an individual may be held criminally liable.[10]

---

tions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II]. In addition, relevant customary international law applies to non-international armed conflicts. Domestic law and international human rights law continue to apply in situations of armed conflict. *See, e.g.,* A.P.V. ROGERS, LAW ON THE BATTLEFIELD 217 (3d ed. 2012). The interaction of human rights law, domestic law and LOAC during an armed conflict is a complex matter that is beyond the scope of this paper. In armed conflict LOAC is the *lex specialis*.

7. *See infra* notes 67 and 68 and accompanying text.

8. The United States considers that it is engaged in an armed conflict with Al Qaeda and its associates that spreads across multiple territories. *See, e.g.,* DOJ White Paper, *supra* note 1, at 3. This is not to suggest that the whole world is the battlefield for this type of conflict, but that the conflict spans multiple States. *See, e.g.,* the U.S. Navy, U.S. Marine Corps & U.S. Coast Guard, NWP 1-14M/MCWP 5-12.1/COMDTPUB P5800.7A, The Commander's Handbook on the Law of Naval Operations ¶ 5.1.2.3 (2007), *available at* http://www.usnwc.edu/getattachment/a9b8e92d-2c8d-4779-9925-0defea93325c/1-14M ("The Global War on Terror is an example of this new type of conflict . . . . What law applies in this type of conflict is still being settled.").

9. The terms law enforcement situation and peacetime are not used in this article to mean a total lack of hostilities, but merely to describe situations that do not rise to the level of armed conflicts.

10. THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 618 (Dieter Fleck ed., 2d ed. 2010). Therefore, if hostilities qualify as an armed conflict, targeting an individual participating in the conflict is likely to be lawful (if, of course, it is done in accordance with the applicable rules). In contrast, if considered a law enforcement scenario, the use of force against an individual would be lawful in a more limited set of circumstances. In addition, substantial differences in the content of certain IAC and NIAC rules exist. For example, combatant status and prisoner of war status only pertain to IACs.

Several approaches have been put forth for how to legally categorize extraterritorial hostilities with armed groups. In Part II, this article provides a contextual framework for the discussion by laying out these various approaches. Part III outlines the law applicable to NIACs. Part IV discusses why the prevailing view is that some of these extraterritorial conflicts may qualify as NIACs despite the fact that such conflicts do not conform to the traditional interpretations limiting the application of LOAC to within a State's own borders.[11]

Part V examines potential problems in applying a body of law that was intended for internal application to an extraterritorial context. The fact that the law was not designed for such use has led to inconsistencies in the rationale for when and where this body of law applies. Today, many argue that NIAC law may apply to spill-over conflicts and even to hostilities that occur between a State and an armed group predominantly in the territory of a second uninvolved State (e.g., the Israeli-Hezbollah conflict). In contrast, a great deal of unease surrounds the notion that a global armed conflict is taking place with Al Qaeda. There is concern that the removal of territorial restrictions when establishing the existence of an armed conflict could transform the entire world into a potential "battlefield."[12]

An examination of the requirements for the existence of an armed conflict and their underlying purpose suggest that the criteria for establishing when a NIAC exists cannot be entirely divorced from geography. In particular, difficulties may arise in establishing that an armed conflict exists when hostilities with armed groups span multiple States. One challenge is

---

11. GC III COMMENTARY, *supra* note 5, at 37; Roy S. Schondorf, *Extra-State Armed Conflicts: Is There a Need for a New Legal Regime*, 37 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 1, 50 (2004); ANTHONY CULLEN, THE CONCEPT OF NON-INTERNATIONAL ARMED CONFLICT IN INTERNATIONAL HUMANITARIAN LAW 49–51 (2010); Arimatsu, *supra* note 2, at 186. UNITED KINGDOM MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT ¶ 15.2 (2004) [hereinafter UK MANUAL].

12. *See, e.g.,* Letter from Human Rights Watch to President Barack Obama Re: Targeted Killings and Unmanned Combat Aircraft Systems (Drones) (Dec. 7, 2010), *available at* http://www.hrw.org/news/2010/12/07/letter-obama-targeted-killings ("While the United States is a party to armed conflicts in Afghanistan and Iraq and could become a party to armed conflicts elsewhere, the notion that the entire world is automatically by extension a battleground in which the laws of war are applicable is contrary to international law."). *See also* Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, *Study on Targeted Killings*, ¶¶ 67, 68, Human Rights Council, U.N. Doc. A/HRC/14/24/Add.6 (May 28, 2010) (by Philip Alston), *available at* http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf

how the law factors in the links between various armed groups when calculating whether the violence has reached a sufficient level of intensity necessary to trigger LOAC. This involves a combination of distinguishing the identifiable party and establishing the intensity requirement. Another issue is whether violence diffused over a number of countries can be amassed in order to reach a total level of intensity. In addition, a shift in the State whose sovereignty is affected could have an impact on the underlying purpose of the intensity criterion.

Part VI briefly considers the separate issue of where LOAC may be applied once the law of armed conflict has been triggered. The question is contentious and at this point unresolved. The article suggests that the most defensible position is that once an armed conflict exists, the law applies to the parties to the conflict even if in another country, but that a number of other factors restrict whether or not an individual may be targeted or detained. Under this view, the key question is whether an armed conflict exists in the first place. The majority of the article concentrates on this former question.

Part VII concludes that although the law applicable to NIACs may apply extraterritorially, the process of establishing when an armed conflict exists is still partially bound geographically by virtue of the intensity requirement. In this sense, the law does not simply follow the parties to the conflict. Because the law was designed with territorial constraints in mind, there is a need for clarification of when the law is to apply extraterritorially.

Before addressing the main issues of this article, two preliminary matters should be highlighted. First, a factual distinction is made between three types of hostilities, all of which fall under the category of "extraterritorial": (1) conflicts within a single State that spill over into neighboring States; (2) conflicts that take place between a State and an armed group located in a second uninvolved State; and (3) conflicts between a State and an armed group that spread across multiple States. Scholars frequently use the term "transnational armed conflicts" to describe the latter two situations,[13] and

13. *See, e.g.,* Geoffrey Corn & Eric T. Jensen, *Transnational Armed Conflict: A 'Principled' Approach to the Regulation of Counter-Terror Combat Operations*, 42 ISRAEL LAW REVIEW 46 (2009), *available at*: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1256380 [hereinafter Corn & Jensen, *Transnational Armed Conflict*]; Geoffrey Corn, *Hamdan, Lebanon, and the Regulation of Hostilities—The Need to Recognize a Hybrid Category of Armed Conflict*, 40 VANDERBILT JOURNAL OF INTERNATIONAL LAW 295 (2007) [hereinafter Corn, *Hamdan, Lebanon, and the Regulation of Hostilities*]. Other terms used include "extra-state hostilities," Schondorf, *supra* note 11, and "extra-territorial NIAC," Arimatsu, *supra* note 2, at 183.

at times all three.[14] This article employs the terms "spill-over," "cross-border" and "global" armed conflicts, respectively, in order to differentiate between the three types of conflicts.[15]

Second, determining if and when force may be used in self-defense is a different issue than establishing whether that use of force amounts to an armed conflict. The former is a *jus ad bellum* issue and the latter a matter of *jus in bello*. *Jus ad bellum* determines, *inter alia*, under what circumstances a State may use force in self-defense.[16] *Jus in bello* is another name for the body of law applicable to armed conflict. While both are often discussed within the context of extraterritorial hostilities with armed groups and at times conflated,[17] they are distinct bodies of law. Once a State employs force in self-defense, the question still remains as to what body of law governs that use of force. If the situation rises to the level of an armed conflict, LOAC applies.[18] Alternatively, the situation is governed by a law enforce-

---

14. *See generally* Claus Kress, *Some Reflections on the International Legal Framework Governing Transnational Armed Conflict*, 15 JOURNAL OF CONFLICT AND SECURITY LAW 245 (2010).

15. It must be emphasized that these terms refer to factual, not legal, categories of conflict. For a more extensive typology of non-international armed conflicts, see INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERNATIONAL HUMANITARIAN LAW AND THE CHALLENGES OF CONTEMPORARY ARMED CONFLICTS 9–12 (2011), *available at* http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf [hereinafter 31st ICRC Conference on IHL CHALLENGES].

16. *Jus ad bellum* governs the legality of resort to the use of force by a State. The exceptions to the UN Charter's prohibition on the resort to force are individual and collective self-defense, and when authorized by the Security Council under Chapter VII (such as occurred in the military intervention in Libya in 2011).

17. A number of statements by U.S. government officials, for instance, leave it unclear whether the legal justification for using force against Al Qaeda and its associates is that of self-defense, a global armed conflict or both. *See, e.g.,* Harold Hongju Koh, Legal Adviser, U.S. Department of State, Address at Annual Meeting of the American Society of International Law: The Obama Administration and International Law (Mar. 25, 2010), http://www.state.gov/s/l/releases/remarks/139119.htm ("as a matter of international law, the United States is in an armed conflict with al-Qaeda, as well as the Taliban and associated forces, in response to the horrific 9/11 attacks, and may use force consistent with its inherent right to self-defense under international law"). See also Attorney General Eric Holder's response to Senator Lindsey Graham. *Oversight of the U.S. Department of Justice: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 33 (2011) ("The operation against bin Laden was justified as an act of national self defense. It is lawful to target an enemy commander in the field. We did so, for instance, with regard to Yamamoto in World War II when he was shot down in an airplane.").

18. It should be noted that even if LOAC applies and a State has a right to act in self-defense, the question remains as to whether the State using force in self-defense may vio-

ment regime. This article limits its focus to the *jus in bello* issues—specifically, when LOAC applies to extraterritorial hostilities with armed groups.

II. APPROACHES TO APPLYING THE LAW OF ARMED CONFLICT TO EXTRATERRITORIAL HOSTILITIES

Generally, those who view the application of NIAC law as limited to internal armed conflicts maintain that extraterritorial hostilities may still be classified as an armed conflict.[19] They differ, however, in how they characterize the armed conflict. Four main approaches have been put forth for how extraterritorial hostilities between States and armed groups can be classified under the law of armed conflict.

Some, like the Bush administration in its initial position after 9/11,[20] have claimed that these armed conflicts fall entirely outside of the Geneva Conventions. The administration reasoned that because Article 3 Common

late another State's sovereignty in order to do so—also an issue of *jus ad bellum*. This matter involves two competing rights: the right of the territorial State to its sovereignty (and, as such, to its territorial integrity) and the right of the victim-State to defend itself. If the territorial State is unwilling or unable to police the matter itself, then some argue that State loses partial right to its territorial integrity. The "unable and unwilling" test is taken from the law of neutrality found in three of the 1907 Hague Conventions. *See* Convention No. 5 Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct.18, 1907, 36 Stat. 2310; Convention No. 11 Relative to Certain Restrictions with Regard to the Exercise of the Right of Capture in Naval War, Oct. 18, 1907, 36 Stat. 2396; Convention No. 13 Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415. For some suggested criteria to determine when a State might be considered unwilling or unable, see Ashley Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extra-Territorial Self-Defense,* 52 VIRGINIA JOURNAL OF INTERNATIONAL LAW 483 (2011). Issues of sovereignty do not arise if the territorial State gives consent to the victim-State. However, the basis for which a victim-State can use force in the territory of another State in the absence of consent is currently a controversial aspect of international law. These issues are beyond the scope of this article.

19. Schondorf, *supra* note 11, at 30. A minority of commentators, however, consider that the extraterritorial application of violence must be governed by a law enforcement regime. *See, e.g.*, Leila Sadat, *Terrorism and the Rule of Law*, 3 WASHINGTON UNIVERSITY GLOBAL STUDIES LAW REVIEW 135, 140–41 (2004). Schondorf cites a number of commentators who hold this view in *Extra-State Armed Conflicts*, *supra* note 11, at 14−15.

20. *See* Memorandum from George Bush to Vice President et al., Humane Treatment of al Qaeda and Taliban Detainees (Feb. 7, 2002); Memorandum from John C. Yoo & Robert Delahunty to William J. Haynes II, General Counsel, Department of Defense, Re: Application of Treaties and Laws to al Qaeda and Taliban Detainees (Jan. 9, 2002).

to the Geneva Conventions (Common Article 3) only applies within the territory of a State, the hostilities with Al Qaeda could not be categorized as a non-international armed conflict. At the same time, because the conflict did not occur between two States, it could not qualify as an international armed conflict. The position that the conflict with Al Qaeda fell outside the purview of the Geneva Conventions was widely criticized around the world[21] and rejected by the U.S. Supreme Court in *Hamdan*.[22] Given the far-reaching and explicit denunciation of this option, it cannot be seen as a viable approach.

Another view suggests that all conflicts that cross a border must qualify as international armed conflicts, even if one of the parties to the conflict is an armed group. The Israeli Supreme Court took this position in its 2006 Targeted Killing case.[23] Not all Israeli government statements, however, have endorsed the same view.[24] Moreover, apart from the Israeli Supreme Court decision, few other States or commentators share this interpretation.[25] The position contradicts the generally accepted understanding that

---

21. *See, e.g.,* Thom Shanker & Katharine Q. Seelye, *Behind-the-Scenes Clash Led Bush to Reverse Himself on Applying Geneva Conventions*, NEW YORK TIMES (Feb. 22, 2002), at A12, *available at* http://www.nytimes.com/2002/02/22/world/nation-challenged-captives-behind-scenes-clash-led-bush-reverse-himself-applying.html ("Senior officials also disclosed for the first time that NATO allies were so concerned with Mr. Bush's initial decision to reject the conventions that Britain and France warned they might not turn over Taliban and Al Qaeda fighters captured by their troops in Afghanistan unless Mr. Bush pledged to honor the treaties.").

22. Hamdan v. Rumsfeld, 548 U.S. 557 (2006). *See also* John B. Bellinger III, State Department Legal Advisor, Foreign Press Center Briefing: Military Commissions Act of 2006 (Oct. 19, 2006), audio *available at* http://2002-2009-fpc.state.gov/74786.htm.

23. HCJ 769/02 Public Committee against Torture in Israel v. Government of Israel 2006 ¶ 18, (2) PD 459 [2006] (Isr.), *reprinted in* 46 INTERNATIONAL LEGAL MATERIALS 373 (2007), *available at* http://elyon1.court.gov.il/files_eng/02/690/007/a34/02007690.a34.pdf.

24. *See, e.g.,* ISRAEL MINISTRY OF FOREIGN AFFAIRS, THE OPERATION IN GAZA: FACTUAL AND LEGAL ASPECTS ¶ 29 (2009), *available at* http://www.mfa.gov.il/NR/ rdonlyres/E89E699D-A435-491B-B2D0-017675DAFEF7/0/GazaOperationwLinks.pdf ("It is not yet settled which regime applies to cross-border military confrontations between a sovereign State and a non-State terrorist armed group operating from a separate territory.").

25. The International Criminal Court in *Prosecutor v. Thomas Lubanga Dyilo*, Case No. ICC-01/04-01/06-2842, Judgment, ¶ 541 (Mar. 14, 2012), explicitly states that extraterritorial conflicts are not international unless the armed group is acting under the control of the State. *See also* International Committee of the Red Cross, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 89 INTERNATIONAL REVIEW OF THE RED CROSS 719, 725 (2007) [hereinafter ICRC 2007 Report on IHL and the Challenges of Con-

international armed conflicts only occur between States, with the exception of the rare circumstances in which Article 1(4) of Additional Protocol I (AP I) applies or a belligerency is recognized. Although the holding of the Israeli Supreme Court could be used as evidence of emerging customary international law, there would need to be far more indications of State practice and *opinio juris* in order for this position to develop into a customary norm. In addition, this view leaves open the question of whether the full gamut of the Geneva Conventions would apply in the same manner as they would to inter-State conflicts.

Still others have maintained that because extraterritorial conflicts with armed groups do not fit into the traditional categories of IACs or NIACs, a new category of conflict should be created.[26] Under this view the legal principles applicable in NIACs and IACs could be adopted and tailored to suit extraterritorial conflicts,[27] however, it is not clear exactly what rules would apply or what threshold would trigger such conflicts. While proponents acknowledge that their view does not reflect the current state of the law, they suggest that it constitutes *lege ferenda*.[28] This position has been countered in recent years by developments in jurisprudence, the practice of States and an increasing number of scholars.[29]

The final alternative put forth—and one increasingly gaining acceptance—is that Common Article 3 and relevant customary international law pertaining to NIACs may be applied to extraterritorial conflicts. Those who hold this view do not consider it necessary to create a new category of conflict.[30] Rather, they maintain that the existing law may be interpreted to

---

temporary Armed Conflict]. However, for support that such conflicts are international, see Dapo Akande, *Classification of Armed Conflicts Relevant Legal Concepts*, *in* INTERNATIONAL LAW AND THE CLASSIFICATION OF CONFLICTS 32, 73–74, 77−78 (Elizabeth Wilmshurst ed., 2012).

26. Schondorf, *supra* note 11 at 50−51. Corn, *Hamdan, Lebanon, and the Regulation of Armed Conflict*, *supra* note 13.

27. Schondorf, *supra* note 11 at 5−7, 10, 48; Corn, *Hamdan, Lebanon, and the Regulation of Armed Conflict*, *supra* note 13; Corn & Jensen, *Transnational Armed Conflict*, *supra* note 13, at 5.

28. *See, e.g.,* Schondorf , *supra* note 11, at 9.

29. *See, e.g.*, Jelena Pejic, *The Protective Scope of Common Article 3: More than Meets the Eye*, 93 INTERNATIONAL REVIEW OF THE RED CROSS 16 (2011); 31st ICRC Conference on IHL CHALLENGES, *supra* note 15 ("There does not appear to be, in practice, any current situation of armed violence between organized parties that would not be encompassed by one of the two classifications . . . ."); Akande, *supra* note 25, at 71; NOAM LUBELL, EXTRATERRITORIAL USE OF FORCE AGAINST NON-STATE ACTORS 127, 128 (2010).

30. For a detailed assessment of why, in general, the existing regimes of either law en-

apply extraterritorially. This approach thus moves away from the traditional understanding that the applicability of Common Article 3 is limited to internal armed conflicts. Today, this standpoint reflects the predominant trend. It was the position taken by the U.S. Supreme Court in *Hamdan* and has been advanced by numerous commentators.[31]

In sum, there is currently very little law or practice to support the first three options (that the Geneva Conventions do not apply, IAC law applies or a third category of conflict should be created). What is more, the fourth option (that NIAC law may apply extraterritorially) has garnered widespread support. As such, this article focuses on the fourth view.

III. EXISTENCE OF A NON-INTERNATIONAL ARMED CONFLICT

Two types of non-international armed conflicts can be found in treaty law: those governed by Common Article 3 and those to which Additional Protocol II (AP II) applies.[32] Importantly for the purposes of this article, Common Article 3 has a lower threshold of applicability than does AP II.[33] Its application therefore reflects the dividing line between situations of law enforcement and those of armed conflict. Not all hostilities amount to an armed conflict. Common Article 3 distinguishes between mere internal disturbances and tensions and those situations that rise to the level of an

---

forcement or NIAC are sufficient, see Marco Sassòli, *Transnational Armed Groups and International Humanitarian Law* 25, 6 HPCR OCCASIONAL PAPER SERIES (Winter 2006). *See also* SANDESH SIVAKUMARAN, THE LAW OF NON-INTERNATIONAL ARMED CONFLICT 228–29 (2012).

31. *See, e.g.*, Marco Sassòli, *Use and Abuse of the Laws of War*, 22 LAW AND INEQUALITY 195, 201(2004); SIVAKUMARAN, *supra* note 30, at 229.

32. Some debate exists as to whether the Rome Statute of the International Criminal Court establishes a third threshold of non-international armed conflict. However, the drafting history, jurisprudence and majority of scholars do not support this view. Rome Statute of the International Criminal Court arts. 8(2)(d), 8(2)(f), July 17, 1998, 2187 U.N.T.S. 90. *See, e.g.*, Prosecutor v. Limaj, Case No. IT-03-66-T, Judgment, ¶ 87 (Int'l Crim. Trib. for the former Yugoslavia Nov. 30, 2005); Dino Kritsiotis, *The Tremors of Tadić*, 43 ISRAEL LAW REVIEW 262, 288 (2010); Theodor Meron, *The Humanization of Humanitarian Law*, 94 AMERICAN JOURNAL OF INTERNATIONAL LAW 239, 260–61 (2000); Anthony Cullen, *The Definition of Non-International Armed Conflict in the Rome Statute of the International Criminal Court: An Analysis of the Threshold of Application Contained in Article 8(2)(f)*, 12 JOURNAL OF CONFLICT AND SECURITY LAW 419 (2007).

33. A key distinguishing factor between the two regimes is that Article 1 of AP II requires armed groups to have the ability to control territory.

armed conflict.[34] Internal disturbances are not regulated by Common Article 3, but instead are controlled by law enforcement rules, human rights and other applicable law. It is only once the threshold of an armed conflict is reached that Common Article 3 applies.

Customary international law is particularly relevant in NIACs, given the dearth of treaty law rules. This article takes the position that the criteria triggering the application of Common Article 3 are the same as those required by customary international law to establish the existence of a NIAC. To conclude otherwise would create an additional category of conflict, an outcome that is generally rejected. The move in both treaty law and jurisprudence towards making fewer distinctions in types of NIACs, rather than more,[35] lends credence to viewing the Common Article 3 and customary law thresholds of armed conflict as synonymous.

Common Article 3, widely considered to reflect customary international law,[36] governs non-international armed conflicts between a State(s) and armed group(s), as well as those conflicts between armed groups.[37] The full Article reads as follows:

> In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply, as a minimum, the following provisions:

---

34. The phrase "internal tensions and disturbances" is shortened to "internal disturbances" throughout the article for clarity's sake. Although taken from AP II, Article 1(2), and not explicitly found in Common Article 3, the rule is widely understood to be applicable to Common Article 3. *See* COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949*,* ¶¶ 4472−73 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987) [hereinafter AP II COMMENTARY]; Prosecutor v. Jean-Paul Akayesu, Case No. ICTR-96-4-T, Judgment, ¶¶ 620, 625 (Sept. 2, 1998); *Limaj* Trial Judgment, *supra* note 32, ¶ 84; Rome Statute, *supra* note 32, art. 8(2)d; UK MANUAL, *supra* note 11, ¶ 15.2.1; THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW, *supra* note 10, at 616; International Committee of the Red Cross, *How is the Term "Armed Conflict" Defined in International Humanitarian Law?* 3 (2008), *available at* http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf.

35. *See, e.g.*, Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict art. 22, Mar. 26, 1999, 2253 U.N.T.S. 212. *See generally* CUSTOMARY INTERNATIONAL HUMANITARIAN LAW (2 volumes) (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005) [hereinafter CIHL Study].

36. *Akayesu* Trial Judgment, *supra* note 34, ¶ 608; *Tadić* Appeals Decision on Jurisdiction, *supra* note 5, ¶¶ 116, 134; Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶ 218 (June 27) [hereinafter ICJ *Nicaragua* Case].

37. AP II COMMENTARY, *supra* note 34, ¶ 4461. THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW, *supra* note 10, at 609.

> (1) Persons taking no active part in the hostilities, including members of armed forces who have laid down their arms and those placed "hors de combat" by sickness, wounds, detention, or any other cause, shall in all circumstances be treated humanely, without any adverse distinction founded on race, colour, religion or faith, sex, birth or wealth, or any other similar criteria. To this end, the following acts are and shall remain prohibited at any time and in any place whatsoever with respect to the above-mentioned persons:
>
> (a) violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;
>
> (b) taking of hostages;
>
> (c) outrages upon personal dignity, in particular humiliating and degrading treatment;
>
> (d) the passing of sentences and the carrying out of executions without previous judgment pronounced by a regularly constituted court, affording all the judicial guarantees which are recognized as indispensable by civilized peoples.
>
> (2) The wounded and sick shall be collected and cared for. An impartial humanitarian body, such as the International Committee of the Red Cross, may offer its services to the Parties to the conflict. The Parties to the conflict should further endeavour to bring into force, by means of special agreements, all or part of the other provisions of the present Convention. The application of the preceding provisions shall not affect the legal status of the Parties to the conflict.

Common Article 3 provides minimum standards for humane treatment of persons no longer taking part in hostilities. In addition, as a result of developments in customary international law, once Common Article 3 is triggered, a number of LOAC rules governing the conduct of hostilities are also applicable.[38] Strong support exists among commentators, jurisprudence and State practice for this interpretation,[39] reinforcing the position

38. Whether one views that it is the application of conduct of hostilities rules to conflicts that have been triggered by Common Article 3, or that Common Article 3 is itself now interpreted to include conduct of hostilities rules, is not material to this analysis.

39. Article 8(2)e of the Rome Statute supports the customary law status of some conduct of hostilities rules in NIACs. *See also* Prosecutor v. Blaskić, Case No. IT-95-14-T, Judgment, ¶ 170 (Int'l Crim. Trib. for the former Yugoslavia Mar. 3, 2000); Prosecutor v. Kordić and Čerkez, Motion to Dismiss the Amended Indictment for Lack of Jurisdiction

that the threshold for Common Article 3's applicability is synonymous with that of a non-international armed conflict. Disagreement, however, exists as to exactly which rules on the conduct of hostilities reflect customary international law.[40]

As has been frequently pointed out, despite the important consequences resulting from its application, Common Article 3 does not specify when a situation amounts to an armed conflict.[41] Three explicit requirements necessary to trigger Common Article 3 can be found in treaty law: (1) the existence of an armed conflict, (2) the armed conflict is not of an international character and (3) the armed conflict takes place in the territory of

---

Based on the Limited Jurisdictional Reach of Articles 2 and 3, ¶ 30 (Int'l Crim. Trib. for the former Yugoslavia Mar. 2, 1999). In addition, some recent conventions, which place limits on methods and means of warfare, apply to both IACs and NIACs. *See, e.g.*, Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Oct. 10, 1980, 1342 U.N.T.S. 137; Second Protocol to the Hague Convention, *supra* note 35, art. 22; Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, Apr. 10, 1972, 26 U.S.T. 583, 1015 U.N.T.S. 163; Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, Jan. 13, 1993, 1974 U.N.T.S. 45. *See also* THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW, *supra* note 10, at 614−16, 624−25; Robin Geiss, *Armed Violence in Fragile States: Low-Intensity Conflicts, Spillover Conflicts, and Sporadic Law Enforcement Operations by Third Parties*, 91 INTERNATIONAL REVIEW OF THE RED CROSS 127, 133–34 (2009).

40. The ICRC's customary international law study, for instance, suggests that 147 of the 161 rules contained in the study are applicable in both international and non-international armed conflicts. CIHL Study, *supra* note 35. *But see* Letter from John Bellinger III, Legal Adviser, U.S. Department of State, & William J. Haynes, General Counsel, U.S. Department of Defense, to Dr. Jakob Kellenberger, President, International Committee of the Red Cross, Regarding Customary International Law Study (Nov. 3, 2006), *reprinted in* 46 INTERNATIONAL LEGAL MATERIALS 514 (2007). The *Tadić* Appeals Decision on Jurisdiction, *supra* note 5, ¶ 127, states that customary rules applicable in NIACs include the "protection of civilians . . . from indiscriminate attacks, protection of civilian objects, in particular cultural property, protection of all those who do not (or no longer) take active part in hostilities, as well as prohibition of means of warfare proscribed in inter-national armed conflicts and ban of certain methods of conducting hostilities."

41. *See, e.g.,* Prosecutor v. Musema, Case No. ICTR-96-13-A, Appeals Judgment, ¶¶ 246, 252 (Jan. 27, 2000); 1 MARCO SASSÒLI & ANTOINE A. BOUVIER, HOW DOES LAW PROTECT IN WAR 109 (2d ed. 2011); LINDSEY MOIR, THE LAW OF INTERNAL ARMED CONFLICT 31 (2002); COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 34, ¶¶ 4448, 4450. Interestingly, the ICRC customary international law study does not address the criteria for the existence of a non-international armed conflict. CIHL STUDY, *supra* note 35.

one of the high contracting parties.[42] In addition, although not explicit in the text, hostilities must surpass situations of internal disturbances in order for an armed conflict to exist.[43] In any case, the existence of an armed conflict is determined through an assessment of the facts on the ground.[44]

The ambiguity surrounding Common Article 3's threshold of application can be traced back to its codification in 1949. The groundbreaking inclusion of non-international armed conflicts in the regulatory framework of violence reflected a delicate compromise between States' sovereign concerns and the interests of humanity. The implicit exclusion of situations of internal disturbances from the purview of Common Article and the lack of clarity as to the threshold of the law's applicability were a consequence of these underlying tensions. Governments traditionally have feared intrusion into their sovereign affairs. They considered the regulation by international law over their internal matters to be an incursion in their sovereignty that could affect their ability to maintain law and order and impact the national security of the State. States have also long been reluctant to grant any appearance of legitimacy to armed groups rebelling against their authority.[45] As a consequence of these factors, States considered that the violence had to reach a certain threshold—beyond internal disturbances—in order to justify what they considered to be interference in their internal affairs. Moreover, the lack of clarity as to Common Article 3's threshold was seen to be beneficial as it offered flexibility to States to deny the existence of an armed conflict.[46]

Humanitarian interests also played a role in requiring that the threshold surpass situations of internal disturbances. One of the underlying purposes of Common Article 3 is to bring a body of law into effect when the normal

---

42. Common Article 3: "In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties . . . ."

43. *See supra* note 34 and accompanying text.

44. *See, e.g.*, Prosecutor v. Rutaganda, Case No. ICTR-96-3-T, Judgment and Sentence, ¶ 93 (Dec. 6, 1999); *Limaj* Trial Judgment, *supra* note 32, ¶ 93; CULLEN, *supra* note 11, at 131−32.

45. This concern resulted in the last paragraph of Common Article 3 stating: "The application of the preceding provisions shall not affect the legal status of the Parties to the conflict." *See also* AP II, *supra* note 6, art. 3(2).

46. In fact, Common Article 3's application has been frequently contested. The U.S. government, for instance, initially denied Common Article 3's applicability to Al Qaeda after 9/11. *See* Meron, *supra* note 32, at 261 n.117; RENÉ PROVOST, INTERNATIONAL HUMAN RIGHTS AND HUMANITARIAN LAW 268 (2002). These authors provide a number of examples where States have denied Common Article 3's applicability. *See also* G.I.A.D. Draper, *The Geneva Conventions of 1949*, 114(I) RECUEIL DES COURS 57, 87–88 (1965).

system of law and order breaks down.[47] For this reason, a distinction was made between internal disturbances and situations of armed conflict. The ambiguity surrounding the application of Common Article 3 was considered positive by some as it allowed for the necessary flexibility to deal with changing circumstances and the expansion of types of situations that could fall under it.[48]

In more recent years, jurisprudence of international tribunals and State practice has provided some clarification for Common Article 3's threshold. Today, Common Article 3 conflicts exist when the hostilities have reached a certain level of intensity and when the armed groups involved are sufficiently organized.[49] These two requirements, known as the *Tadić* test, were first articulated by the International Criminal Tribunal for the former Yugoslavia (ICTY) in the *Tadić* Appeals Chamber judgment: "Armed conflict exists whenever there is a resort to armed force between States *or protracted armed violence* between governmental authorities and *organized armed groups* or between such groups within a State."[50]

The key purpose underlying both criteria is to distinguish situations of internal disturbances from those of armed conflict.[51] This test is now considered to be reflective of customary international law. Subsequent decisions of the ICTY and the International Criminal Tribunal for Rwanda (ICTR) have repeatedly relied on the *Tadić* test.[52] Significantly, States draft-

47. *See, e.g.,* NILS MELZER, TARGETED KILLING IN INTERNATIONAL LAW 256 (2008).

48. *See, e.g.,* Draper, *supra* note 46, at 87; MOIR, *supra* note 41, at 33, 42; CULLEN, *supra* note 11, at 60; Heike Spieker, *Twenty-Five Years After the Adoption of Additional Protocol II: Breakthrough or Failure of Humanitarian Legal Protection?*, 4 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 141 (2001); GC III COMMENTARY, *supra* note 5, at 35.

49. *Tadić* Appeals Decision on Jurisdiction, *supra* note 5, ¶ 70. *See, e.g.,* 31st ICRC Conference on IHL CHALLENGES, *supra* note 15, at 8, 9. Jelena Pejic, *Terrorist Acts and Groups: A Role for International Law?*, 75 BRITISH YEARBOOK OF INTERNATIONAL LAW 86 (2004).

50. *Tadić* Appeals Decision on Jurisdiction, *supra* note 5, ¶ 70 (emphasis added).

51. Prosecutor v. Tadić, Case No. IT-94-1-T ICTY, Judgment, ¶ 562 (Int'l Crim. Trib. for the former Yugoslavia May 7, 1997). *See also*: Prosecutor v. Haradinaj, Case No. IT-04-84-T, Judgment, ¶ 38 (Int'l Crim. Trib. for the former Yugoslavia Apr. 3, 2008); Prosecutor v. Kordić and Čerkez, Case No. IT-95-14/2-A, Appeals Judgment, ¶ 341 (Int'l Crim. Trib. for the former Yugoslavia Dec. 17, 2004); Prosecutor v. Delalić et al., Case No. IT-96-21-T, Judgment, ¶ 184 (Int'l Crim. Trib. for the former Yugoslavia Nov. 16, 1998); *Limaj* Trial Judgment, *supra* note 32, ¶¶ 84, 89; *Akayesu* Trial Judgment, *supra* note 34, ¶ 620. *Musema* Appeals Judgment, *supra* note 41, ¶ 248. Rome Statute, *supra* note 32, art. 8(2)(f).

52. *See, e.g., Akayesu* Trial Judgment, *supra* note 34, ¶ 620. *Rutaganda* Trial Judgment, *supra* note 44, ¶ 93; *Tadić* Trial Judgment, *supra* note 51, ¶¶ 561−62; *Delalić* Trial Judgment, *supra* note 51, ¶¶ 183−85; Prosecutor v. Krnojelac et al., Case No. IT-97-25-T, Judgment,

ing the Rome Statute of the International Criminal Court basically incorporated the *Tadić* test as the definition for the threshold of a NIAC.[53] Various international bodies have turned to the *Tadić* test in order to determine the existence of an armed conflict.[54] Some States, such as the United Kingdom, have explicitly cited the *Tadić* test in their military manuals.[55] Finally, the majority of commentators today refer to the *Tadić* test as a reflection of the current state of law.[56]

Jurisprudence from the ICTY has supplied a number of indicative factors that help to identify when the criteria of intensity and organization have been met. Factors suggesting that the requisite level of organization has been reached include:

(1) the existence of a command structure;
(2) an ability to carry out operations in an organized manner;
(3) the level of logistics;
(4) a level of discipline and ability sufficient to implement the basic obligations of Common Article 3; and
(5) an ability to speak with one voice.[57]

¶ 51 (Int'l Crim. Trib. for the former Yugoslavia Mar. 15, 2002); Prosecutor v. Kunarac et al., Case No. IT-96-23, Appeals Judgment, ¶ 56 (Int'l Crim. Trib. for the former Yugoslavia June 12, 2002); *Kordić* and *Čerkez* Appeals Judgment, *supra* note 51, ¶ 336; *Limaj* Trial Judgment, *supra* note 32, ¶ 84; Prosecutor v. Naletilić, Case No. IT-98-34-T, Judgment, ¶ 225 (Int'l Crim. Trib. for the former Yugoslavia Mar. 31, 2003); *Haradinaj* Trial Judgment, *supra* note 51, ¶¶ 37–38; Prosecutor v. Boškoski and Tarčulovski, Case No. IT-04-82-T, Judgment, ¶ 175 (Int'l Crim. Trib. for the former Yugoslavia July 10, 2008); Prosecutor v. Milosević, Case No. IT-02-54-T, Decision on Motion for Judgment of Acquittal, ¶¶ 18–21 (Int'l Crim. Trib. for the former Yugoslavia Feb. 25, 2004).

53. Rome Statute, *supra* note 32, art. 8(2)(f).

54. *See, e.g.*, International Commission of Inquiry on Darfur, *Report to the United Nations Secretary-General Pursuant to Security Council Resolution 1564 of 18 September 2004*, ¶¶ 74−76, U.N. Doc. S/2005/60 (Jan. 25, 2005).

55. *See, e.g.*, UK MANUAL, *supra* note 11, ¶ 15.3.1. As further evidence of State practice, see the Israeli government's reference to the *Tadić* test, demonstrating that the conflict with Hamas could fulfill the requirements for a NIAC, even though as a matter of policy Israel applies both IAC and NIAC rules to its operations in Gaza. ISRAEL MINISTRY OF FOREIGN AFFAIRS, THE OPERATION IN GAZA: FACTUAL AND LEGAL ASPECTS ¶ 28 (2009).

56. *See, e.g.*, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE rule 23 (Michael N. Schmitt ed., 2013); Michael Cottier, *in* OTTO TRIFFTERER, COMMENTARY ON THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT 291, 292 (2d ed. 2008).

57. *Boškoski* Trial Judgment, *supra* note 52, ¶¶ 199−203, 277. *See also Limaj* Trial

The ICTY jurisprudence establishes the following factors as indicators that the required level of intensity has been reached:

(1) the seriousness, increase and spread of clashes over territory and time;
(2) the distribution and type of weapons;
(3) government forces (number, presence in crisis area and the way force is used);
(4) the number of casualties;
(5) the number of civilians fleeing the combat zone;
(6) the extent of destruction;
(7) blocking, besieging and heavy shelling of towns;
(8) the existence and change of front lines;
(9) occupation of territory;
(10) road closures; and
(11) UN Security Council attention.[58]

While these factors are helpful, it must be highlighted that they are not requirements, but merely indicators. The minimum level of organization and intensity necessary in order for a non-international conflict to be triggered continues to be debated.

It is suggested here that the organized armed group must at least possess a responsible command and have the ability to abide by LOAC. The latter prerequisite can be read into the fact that Common Article 3 requires all parties to the conflict to fulfill certain obligations.[59] In order to satisfy these requirements, the parties must also have the *ability* to abide by the applicable law. The criterion of a responsible command is implicit in

---

Judgment, *supra* note 32, ¶ 90; *Haradinaj* Trial Judgment, *supra* note 51, ¶ 64; *Milosević* Decision, *supra* note 52, ¶ 23; Prosecutor v. Djordjević, Case No. IT-05-87/1-T, Judgment, ¶¶ 1525−26 (Int'l Crim. Trib. for the former Yugoslavia Feb. 23, 2011); *Lubanga* Trial Judgment, *supra* note 25, ¶ 537.

58. The *Boškoski* Trial Judgment, *supra* note 52, ¶ 177. The *Boškoski* Trial Judgment is particularly useful as it summarizes previous ICTY case law as well as a discussion on relevant national court decisions. *Boškoski* Trial Judgment, *supra* note 52, ¶¶ 177−83. *See also Djordjević* Trial Judgment, *supra* note 57, ¶ 1523; *Lubanga* Trial Judgment, *supra* note 25, ¶ 538.

59. Common Article 3: "In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, *each Party to the conflict shall be bound* to apply, as a minimum, the following provisions . . . ." (emphasis added).

Common Article 3, as evidenced by the drafting history,[60] case law[61] and the position taken by the majority of commentators.[62] In addition, the fact that command responsibility is considered applicable to conflicts governed by Common Article 3 as a matter of customary international law today[63] lends support to this interpretation. Command responsibility is premised on, among other things, the existence of a responsible command.[64] Therefore, the customary law status of command responsibility recognizes that a responsible command is a required component for the existence of an armed conflict.

As with the organization requirement, opinions differ with regard to the level of intensity necessary for a situation to amount to a Common Article 3 conflict. In particular, it is debated whether the gravity of the violence or its duration (or protractedness) should be the determinative factor in reaching the necessary intensity threshold for an armed conflict to exist. In the *Abella* case, the Inter-American Commission on Human Rights placed more emphasis on the gravity of a situation over its duration.[65] The

60. *See, e.g.,* GC III COMMENTARY, *supra* note 5, at 36.

61. *See, e.g., Boškoski* Trial Judgment, *supra* note 52, ¶196; Prosecutor v. Hadžihasanović, Case No. IT-01-47-AR72, Appeals Chamber Decision on Interlocutory Appeal Challenging Jurisdiction in Relation to Command Responsibility, ¶ 16 (Int'l Crim. Trib. for the former Yugoslavia July 16, 2003). ICTY judgments vary as to the importance given to the duration factor.

62. *See, e.g.,* MOIR, *supra* note 41, at 36, 43; MICHAEL BOTHE, KARL JOSEF PARTSCH & WALDEMAR A. SOLF, NEW RULES FOR VICTIMS OF ARMED CONFLICTS, COMMENTARY ON THE TWO 1977 PROTOCOLS ADDITIONAL TO THE GENEVA CONVENTIONS OF 1949, at 624–25 (1982).

63. *See, e.g.,* Prosecutor v. Hadžihasanović, Case No. IT-01-47-T, Judgment, ¶¶ 93, 179 (Int'l Crim. Trib. for the former Yugoslavia Mar. 15, 2006). *See also* Statute of the International Criminal Tribunal for Rwanda art. 6(3), S.C. Res. 955, Annex, U.N. Doc. S/RES/955 (Nov. 8, 1994); Statute of the Special Court for Sierra Leone art. 6(3), annexed to Agreement between the United Nations and the Government of Sierra Leone on the Establishment of a Special Court for Sierra Leone, Jan. 16, 2002, 2178 U.N.T.S. 138; Rome Statute, *supra* note 32, art. 28.

64. Although responsible command and command responsibility are two different concepts, they are related. *See, e.g., Hadžihasanović* Appeals Judgment, *supra* note 61, ¶ 16; GUÉNAËL METTRAUX, THE LAW OF COMMAND RESPONSIBILITY 54−55 (2009). Demonstrating command responsibility entails a stricter test than finding that a responsible command exists. *See, e.g., Limaj* Trial Judgment, *supra* note 32, ¶ 89; METTRAUX, *supra*, at 56.

65. The *Abella* case (also referred to as the *Tablada* case) concerns an attack on a military barracks in Argentina by forty-two individuals in 1989. The battle lasted thirty hours and resulted in the death of twenty-nine of the attackers, as well as a number of the State officials. The Inter-American Commission on Human Rights held that this situation constituted an armed conflict governed by Common Article 3 and relevant customary interna-

ICTY jurisprudence has generally held that both aspects matter, although the judgments are not always consistent in the emphasis placed on each factor.[66] The ICTY approach of incorporating both components of intensity seems to be the predominant trend today.

Until recently, the debate surrounding Common Article 3's threshold of applicability paid little attention to the Article's requirements that a conflict be "not of an international character" and take place "in the territory of a High Contracting party." The drafting history and literal meaning of the text of Common Article 3 made clear that Common Article 3 was intended to apply to internal armed conflicts.[67] As a result, over the years States, commentators and jurisprudence have consistently understood the territorial scope of Common Article 3 to be restricted to internal armed conflicts.[68]

This interpretation of Common Article 3 has been challenged in recent years for several reasons. Armed groups have grown in strength and acquired an ability to act against States across multiple borders. At the same time, an increased recognition that internal conflicts often spill over into neighboring countries exists. These developments highlight the inconsistency between traditional State-centric, territorially bound views entrenched in the law of armed conflict and realities on the ground. Moreover, the long-standing resistance of States, which has permeated the development, codification and enforcement of NIAC law, to concede to the ap-

---

tional law. Abella v. Argentina, Case No. 11.137, Inter-Am. Comm'n H.R., Report No.55/97, OEA/Ser/L/V/II.98, doc. 6 rev. ¶156 (1997). For a critique of this case, see Liesbeth Zegveld, *The Inter-American Commission for Human Rights and International Humanitarian Law: A Comment on the* Tablada *Case*, 324 INTERNATIONAL REVIEW OF THE RED CROSS 505 (1998).

66. *See, e.g., Haradinaj* Trial Judgment, *supra* note 51, ¶ 49 ("The criterion of protracted armed violence has therefore been interpreted in practice, including by the *Tadic* Trial Chamber itself, as referring more to the intensity of the armed violence than to its duration."); *Boškoski* Trial Judgment, *supra* note 52, ¶ 186 (stating that the term "protracted" adds a "temporal element to the definition of armed conflict"), ¶ 185 ("In applying this test, what matters is whether the acts are perpetrated in isolation or as part of a protracted campaign that entails the engagement of both parties in hostilities.").

67. GC III COMMENTARY, *supra* note 5, at 37. Schondorf, *supra* note 11, at 50; CULLEN, *supra* note 11, at 49−51.

68. *See, e.g.*, UK MANUAL, *supra* note 11, at 383; GC III COMMENTARY, *supra* note 5, at 37; CULLEN, *supra* note 11, at 49−51. MICHAEL N. SCHMITT, CHARLES H.B. GARRAWAY & YORAM DINSTEIN, THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT WITH COMMENTARY ¶ 1.1.1(a) (2006), *reprinted in* 36 ISRAEL YEARBOOK ON HUMAN (2006) (Special Supplement).

plication of Common Article 3 may be shifting for some States. The United States in its current global armed conflict against Al Qaeda is leading this move towards a wider application, rather than avoidance, of the law of armed conflict.

Some scholars have identified the development of international human rights law and its accompanying restrictions to be an impetus for this shift.[69] They suggest that as a result of the increasing constraints of human rights law, characterizing a situation as one of armed conflict actually allows States more flexibility in how they may lawfully deal with armed groups (in terms of targeting and detention).[70] An additional contributing factor may be that in these situations the majority of the violence does not take place in the territory of the State fighting the armed group, but occurs on a second State's territory. As such, the fear of the fighting State that it might appear to lack an ability to maintain law and order is no longer present. This set of circumstances has evoked reaction and led to renewed debate within the international law community as to the conditions for the applicability of Common Article 3.[71] One of the challenges today is if and how Common Article 3 applies extraterritorially.

IV. EXTRATERRITORIAL APPLICATION OF COMMON ARTICLE 3

The prevailing view today is that Common Article 3 and relevant customary international law may apply to armed conflicts that are not international in character.[72] This view re-interprets the geographic scope of Common Article 3 in accordance with the rules on treaty interpretation found in the Vienna Convention on the Law of Treaties.[73] It is based on a reading of

69. Kress, *supra* note 14, at 260−61; David Krezmer, *Rethinking Application of IHL in Non-international Armed Conflicts*, 42 ISRAEL LAW REVIEW 8 (2009).

70. Kress, *supra* note 14, at 260−61; Krezmer, *supra* note 69, at 8. *See also* 31st ICRC Conference on IHL CHALLENGES, *supra* note 15, at 10 ("It should be borne in mind that IHL rules governing the use of force and detention for security reasons are less restrictive than the rules applicable outside of armed conflicts governed by other bodies of law."). This is not to say that these States have abandoned the concern that acknowledging the existence of an armed conflict might be seen as bestowing legitimacy upon the armed group. The U.S. law that prohibits the provision of "material support" to designated foreign terrorist organizations (18 U.S.C. §§ 2339A, 2339B (2006)), which was upheld in *Holder v. Humanitarian Law Project*, 130 S. Ct. 2075 (2010), is an example of the State's fear of legitimizing various armed groups.

71. *See, e.g.*, Letter from Human Rights Watch, *supra* note 12.

72. That is, any conflict not covered by Common Article 2 or AP I.

73. Vienna Convention on the Law of Treaties, May 23, 1969, 1155 U.N.T.S. 331.

Common Article 3 that corresponds with the text, the object and purpose of the Geneva Conventions,[74] emerging practice of States,[75] judicial decisions and the views of prominent commentators.[76]

The most frequently cited argument in support of this interpretation is that because the Geneva Conventions are universally ratified, the phrase "in the territory of one of the High Contracting Parties" has lost its significance. According to a literal reading of the text, every armed conflict today takes place "in the territory of one of the High Contracting Parties."[77] Moreover, an initial reason for the geographic restriction was to specify that only those States party to the Conventions would be bound by it. This distinction, too, no longer has relevance.[78]

Simultaneously, more emphasis has been placed on the phrase "not of an international character."[79] This was the approach of the Supreme Court in the *Hamdan* decision, where the Court held that "[t]he term 'conflict not of an international character' is used . . . in contradistinction to a conflict

---

74. *Id.*, art. 31, provides that treaties should be interpreted in good faith and in accordance with the ordinary meaning of the text, in the context of the treaty and with regard to its object and purpose.

75. *Id.*, art. 31(3)b, provides that in addition to interpreting a treaty "in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose," "any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation" should be taken into account.

76. *Id.*, art. 32, specifies that supplementary means of interpretation (preparatory work and circumstances surrounding a treaty's codification) may be resorted to when the treaty's meaning is "ambiguous or obscure" or "leads to a result which is manifestly absurd or unreasonable." Article 38 of the Statute of the International Court of Justice refers to judicial decisions and the teachings of the "most highly qualified publicists" as subsidiary means of interpretation. Statute of the International Court of Justice, June 26, 1945, 59 Stat. 1055, 33 U.N.T.S. 993.

77. This is the ICRC position. *See* International Committee of the Red Cross, *How is the Term "Armed Conflict" Defined in International Humanitarian Law?*, (Mar. 17, 2008), http://www.icrc.org/eng/assets/files/other/opinion-paper-armed-conflict.pdf. *See also* MOIR, *supra* note 41, at 31; Sylvain Vité, *Typology of Armed Conflicts in International Humanitarian Law: Legal Concepts and Actual Situations*, 91 INTERNATIONAL REVIEW OF THE RED CROSS 69, 90 (2009). In addition, the drafting history, while clearly focused on purely internal armed conflicts, does not explicitly rule out the extraterritorial application of Common Article 3. Pejic, *supra* note 29, at 12, 13; LIESBETH ZEGVELD, ACCOUNTABILITY OF ARMED OPPOSITION GROUPS IN INTERNATIONAL LAW 136 (2002); SIVAKUMARAN, *supra* note 30, at 229, 230.

78. *See, e.g.*, Sassòli, *supra* note 30, at 9; SIVAKUMARAN, *supra* note 30, at 229; TALLINN MANUAL, *supra* note 56, cmt. to rule 23, ¶ 3.

79. *See, e.g.*, MELZER, *supra* note 47, at 259.

between nations."[80] As a result of this decision, the United States' position today is that it is engaged in a global conflict with Al Qaeda and its associates governed by Common Article 3.[81]

In addition, restricting application of Common Article 3 to conflicts occurring within State borders does not comport with the object and purpose of the Article. Such an interpretation could result in a gap in protection of the vulnerable. For example, in a spill-over conflict this position essentially means that a "party's humanitarian law obligations would stop at the border,"[82] even though the hostilities and need for the law would not necessarily cease at that point. This gap in protection "could not be explained by States' concerns about their sovereignty."[83] The ICRC's position

---

80. *Hamdan*, *supra* note 22, ¶ 67. The Supreme Court also held that Common Article 3 "is distinguishable from the conflict described in Common Article 2 chiefly because it does not involve a clash between nations (whether signatories or not). In context, then, the phrase 'not of an international character' bears its literal meaning." *Id.*

81. *See, e.g.,* DOJ White Paper, *supra* note 1, at 3 ("The United States is currently in a non-international armed conflict with al-Qaeda and its associated forces."); Memorandum from the Secretary of Defense to the Secretaries of the Military Departments et al. on the Application of Common Article 3 of the Geneva Conventions to the Treatment of Detainees in the Department of Defense 1 (July 7, 2006), *available at* http://www.defense.gov/pubs/pdfs/DepSecDef%20memo%20on%20common%20article%203.pdf ("The Supreme Court has determined that Common Article 3 to the Geneva Conventions of 1949 applies as a matter of law to the conflict with Al Qaeda."); Human Rights Council, United States of America, National Report Submitted in Accordance with Paragraph 15(a) of the Annex to Human Rights Council Resolution 5/1, ¶ 84, U.N. Doc. A/HRC/WG.6/9/USA/1 (Aug. 23, 2010). It should be noted that a number of official statements demonstrate that the United States views itself as being in an armed conflict with Al Qaeda without specifying whether that conflict is an IAC or NIAC. *See, e.g.,* Koh, *supra* note 17, at 14; John Brennan, Assistant to the President for Homeland Security and Counterterrorism, Remarks at Harvard Law School: Strengthening Our Security by Adhering to Our Values (Sept. 16, 2011), *available at* http://www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an [hereinafter Brennan Speech at Harvard]; THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 2, 3 (2011), *available at* http://www.whitehouse.gov/sites/default/files/ counterterrorism_strategy.pdf [hereinafter NATIONAL STRATEGY FOR COUNTERTERRORISM]. *See also* John Bellinger, *Armed Conflict with Al Qaeda?*, OPINIO JURIS (Jan. 15, 2007), http://opiniojuris.org /2007/01/15/armed-conflict-with-al-qaida/.

82. *See* Jelena Pejic, *Status of Armed Conflicts*, *in* PERSPECTIVES ON THE ICRC STUDY ON CUSTOMARY INTERNATIONAL HUMANITARIAN LAW 87 (Elizabeth Wilmshurst & Susan Breau eds., 2007); Pejic, *supra* note 29, at 6; Pejic, *supra* note 49, at 85; Sassòli, *supra* note 30, at 9.

83. Sassòli, *supra* note 30, at 9.

is that Common Article 3 continues to bind both parties to the conflict, even if a border is crossed, as occurs in spill-over and cross-border conflicts.[84] Several judicial developments also point to the applicability of Common Article 3 extraterritorially. The ICTR Statute, for example, includes jurisdiction over crimes committed across the Rwandan border in neighboring countries.[85] This suggests that the parties to the conflict, rather than the territorial boundaries, determine the geographic reach of Common Article 3.[86]

In sum, although it cannot be said categorically that Common Article 3 applies extraterritorially as a matter of customary international law,[87] the prevailing view maintains that Common Article 3 and relevant customary international law can govern extraterritorial hostilities. A consequence of this interpretation is an emphasis on the parties to the conflict, reducing the importance of territory.[88]

V. ORGANIZATION, INTENSITY, AND EXTRATERRITORIALITY—GAPS AND INCONSISTENCIES

Assuming that the law applicable to NIACs can govern extraterritorial hostilities, the question then arises as to how this reduction of the territorial element might impact the conditions widely considered necessary to establish the existence of an armed conflict. Specifically, does this extension of the law's application have an effect on how the organization and intensity requirements apply to extraterritorial hostilities?

It is well accepted that the application of Common Article 3 requires the parties to the conflict be organized and the intensity of the conflict reach a certain level.[89] This test must also be used in determining whether Common Article 3 applies extraterritorially.[90] To conclude otherwise would essentially signify the creation of a third legal category of non-international armed conflicts, entailing the establishment of an additional threshold of

84. 31st ICRC Conference on IHL CHALLENGES, *supra* note 15, at 9, 10.

85. Statute of the International Criminal Tribunal for Rwanda, *supra* note 63, arts. 1, 7.

86. ZEGVELD, *supra* note 77, at 136; Sassòli, *supra* note 30, at 9.

87. Pejic, *supra* note 29, at 17.

88. SIVAKUMARAN, *supra* note 30, at 232.

89. *See supra* note 49 and accompanying text.

90. Leading commentators and judgments from the international tribunals support this view. *See, e.g.*, Marco Sassòli, *The Status of Persons Held in Guantanamo under International Humanitarian Law*, 2 JOURNAL OF INTERNATIONAL CRIMINAL JUSTICE 96, 99–100 (2004); Kress, *supra* note 14, at 261; Pejic, *supra* note 49, at 86, 87.

application and clarification of what rules would then apply. Generating a new category of conflict contradicts the current trend in LOAC toward either reducing the types of NIACs or accepting the existing categories found in Common Article 3 and AP II.[91]

Despite an acknowledgment that Common Article 3 and relevant customary international law can apply extraterritorially, the majority of interpretations do not assess the territorial scope of Common Article 3 together with the organization and intensity requirements. For example, the *Hamdan* decision notably does not refer to the organization and intensity criteria, although it embraces the extraterritorial application of Common Article 3. The *Tadić* test, as developed in ICTY jurisprudence, does not seem to have envisioned extraterritorial hostilities.[92] This is not to suggest that the organization and intensity requirements do not apply to extraterritorial hostilities, but rather to question how they apply. Given that the LOAC system has traditionally been structured territorially, are there any consequences to reducing the relevance of State boundaries?

Moreover, while commentators and States seem to consider that Common Article 3 and the *Tadić* test apply to extraterritorial hostilities, there are inconsistencies in the rationale for the type of extraterritorial conflicts deemed to be covered by NIAC law. Considerable support exists for the position that borders do not matter when establishing Common Article 3 and the *Tadić* test's applicability to spill-over conflicts,[93] and even to cross-border conflicts.[94] The logic, however, seems to change when the discussion turns to "global" conflicts.[95] There appears to be a reluctance to

---

91. *See supra* note 35 and accompanying text.

92. Arimatsu points out that "[f]or the ICTY the only 'geography question' that required clarification was to ascertain the reach of the law *within* the state; the extraterritorial reach of the rules was simply not considered." Arimatsu, *supra* note 2, at 187 (emphasis added). *See also* Robert Chesney, *Who May Be Killed? Anwar al-Awlaki as a Case Study in the International Legal Regulation of Lethal Force*, 13 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 36–37 (2010).

93. HARVARD PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, COMMENTARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE ¶ 2(a)5 (2010) [hereinafter AMW MANUAL COMMENTARY]. *But see* Geiss, *supra* note 39, at 138, for the view that the issue remains unresolved.

94. 31st ICRC Conference on IHL CHALLENGES, *supra* note 15, at 10. Less consensus exists as to how the 2006 conflict between Israel and Hezollah should best be characterized. This uncertainty is compounded by the complexity of the situation. For example, was the conflict internationalized due to overall control of Hezbollah by an outside State?

95. 31st ICRC Conference on IHL CHALLENGES, *supra* note 15, at 10 ("It should be reiterated that the ICRC does not share the view that a conflict of global dimensions is or

accept that Common Article 3 and relevant customary international law may apply to "global" conflicts without regard to State borders.

Part of the criticism involves skepticism that the armed groups in various countries actually form a single party to a distinct conflict. There is also unease with the idea that the law of armed conflict may apply in countries where the level of violence is very low. It seems that territory does still play a role for some commentators,[96] despite acceptance of the extraterritorial application of Common Article 3 and relevant customary international law. In addition, the practice of a number of States does not support the United States' position that territorial boundaries are irrelevant for the application of the law in NIACs.[97] Taken to its logical conclusion, this position would appear to suggest that the organization and intensity criteria should be assessed per territory for "global" conflicts. Yet, it seems inconsistent to maintain on one hand that territorial borders do not stop the application of Common Article 3 to spill-over and cross-border conflicts and, on the other hand, to say that the applicability of Common Article 3 (thus LOAC) must be determined on a case-by-case basis according to territorial constraints with regard to a "global" armed conflict.

An underlying reason for this inconsistency may be the traditional separation of the "protection" and "conduct of hostilities" rules in LOAC. Common Article 3 and the 1949 Geneva Conventions as a whole deal with protective measures (known as "Geneva law"), while the 1907 Hague Regulations concern rules on the conduct of hostilities (known as "Hague law"). It was not until 1977 that the Additional Protocols combined both the "protection" and "conduct of hostilities" rules into one treaty. It may be that the tendency to push for the application of the protective side of the law, while viewing the conduct of hostilities side as too permissive,

---

has been taking place."). *See, e.g.,* Jelena Pejic, *"Unlawful/Enemy Combatants": Interpretations and Consequences*, *in* INTERNATIONAL LAW AND ARMED CONFLICT: EXPLORING THE FAULTLINES: ESSAYS IN HONOUR OF YORAM DINSTEIN 335, 346 (Michael N. Schmitt & Jelena Pejic eds., 2007) (discussing the bombings in Madrid, London, Bali, New Delhi and other places).

96. Sassòli, *supra* note 30 at 8 ("It is not clear to this author why a situation, which is not an armed conflict when it arises on the territory of only one state, should be an armed conflict when it spreads over the territory of several states."). *See also* Pejic, *supra* note 29, at 8, 9.

97. Brennan Speech at Harvard, *supra* note 81. *See also* Kress, *supra* note 14, at 266; Pejic, *supra* note 95, at 346; Sassòli, *supra* note 30, at 10 (referring to the law enforcement response by the Spanish and UK governments to terrorist attacks on their soil in 2004 and 2005).

stems from this traditional division. Although as a matter of black letter law Common Article 3 only contains protection provisions, as noted, once the Article is triggered, so too are the customary rules on conduct of hostilities applicable to NIACs.[98] To separate the two tracks would complicate the application of the law (e.g., what would the threshold of application be for each?).

Setting aside these dual strands in the development of LOAC, an acknowledgment that Common Article 3 and customary international law apply extraterritorially suggests that an assessment of the intensity and organization requirements cannot be conducted separately per country. Even in accepting this conclusion, however, the concern remains that if the territorial restrictions are removed when establishing the existence of an armed conflict over multiple, geographically dispersed States, what constraints within LOAC remain?[99]

It is suggested that territory does still play a role in determining when an armed conflict exists, particularly in the case of "global" armed conflicts. Problems arise if the manner in which the threshold of a NIAC has been determined in internal conflicts is simply transposed to those conflicts that are geographically dispersed across numerous territories. Two issues in particular may challenge the way in which the organization and intensity criteria are applied to "global" armed conflicts. The first concerns the matter of links between armed groups—can violence conducted by various armed groups that are linked to one another be conglomerated in order to fulfill the intensity requirement? If so, what must the nature of the link be? Second, can violence that is dispersed over large geographic spaces be amassed in order to meet the requisite level of intensity for the existence of an armed conflict? In addition, the underlying purpose of the requirements may be affected by a shift in State sovereignty. These factors are now examined.

---

98. *See supra* note 39 and accompanying text.

99. *See, e.g.*, Geiss, *supra* note 39, at 138:

> Clearly, a sweeping and global application of IHL without any territorial confines whatsoever is not maintainable owing to the unjustifiable worldwide derogations from human rights law this would bring about, and in light of the very object and purpose of IHL, i.e. to provide relatively basic but feasible standards in areas where the reality of armed conflict simply forestalls the application of more protective (human rights) standards.

A. Organized Armed Group Criterion

In general, it does not appear that the geographical extension of the law presents insurmountable difficulties for the criterion of an organized armed group in and of itself. The *Tadić* test requires that at least one of the parties consist of an organized armed group. Likewise, a consequence of the extra-territorial application of Common Article 3 is an emphasis on the parties to the conflict over the territorial constraints. In this way, the law of armed conflict can be said to follow the parties to the conflict. This logic can be seen in the widespread understanding today that Common Article 3 applies to spill-over conflicts.[100] Therefore, even if the conflict spans several countries without geographic proximity, there still must be an identifiable party that fulfills the requirements of an organized armed group. Correspondingly, to require that the existence of an organized armed group be separately assessed in each country would not be consistent with the acceptance that the law may apply across State boundaries. The United States, for example, acknowledges the relevance of the organized armed group requirement in conducting its global war on Al Qaeda and its associates.[101]

Where controversy arises is with regard to what constitutes an organized armed group[102] and who is considered to be a member of that group. In particular, the question of whether armed groups organized in networked structures exhibit sufficient organization is crucial for establishing whether an armed conflict exists. Despite its importance, the issue is not specific to the geographical matter discussed here. Similar challenges could arise in the context of a purely internal conflict. At most, it could be argued that large geographical distances may make it more difficult for an armed group to be adequately organized (i.e., possess some of the indicative factors for organization, such as having a command structure and a level of

100. *See, e.g.,* 31st ICRC Conference on IHL CHALLENGES, *supra* note 15, at 9, 10; AMW MANUAL COMMENTARY, *supra* note 93, ¶ 2(a)5; THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW, *supra* note 10, at 605, 607.

101. *See* Koh, *supra* note 17, at 13 (where he mentions that Al Qaeda is an organized armed group). *See also* Jeh Charles Johnson, General Counsel of the U.S. Department of Defense at the Oxford Union, Oxford University: The Conflict Against Al Qaeda and its Affiliates: How Will It End? (Nov. 30, 2012), *available at* http://www.youtube.com/watch?v=cun8o2sDJgE [hereinafter Johnson Oxford Speech].

102. The United States' determination that Al Qaeda is an organized armed group has generated criticism. *See, e.g.*, Noam Lubell, *The War (?) against Al-Qaeda*, *in* INTERNATIONAL LAW AND THE CLASSIFICATION OF CONFLICTS, *supra* note 25, at 421, 425−28 (where he questions who exactly forms the armed group).

discipline that provides an ability to abide by the law). However, the components required for an organized armed group as such, do not change due to a geographical extension of the law's application. Likewise, the location of the conflict does not affect the determination of whether an individual is a member of an organized armed group. While it could be argued that the practical challenges of gathering intelligence in a second State may present additional obstacles to verifying that a particular individual is a group member, the same disputed legal questions on membership that surface in internal conflicts arise wherever the conflict is situated.[103]

B. Party to the Conflict, Conglomeration of Violence and Links between Armed Groups

Particular difficulties may arise in establishing that distinct organized armed groups are part of a single identifiable party. An organized armed group is not necessarily equivalent to a party to the conflict. The party to the conflict may be the organized armed group, it may have an armed wing that constitutes the organized armed group[104] or the party may consist of multiple organized armed groups.[105] With regard to the latter, the law does not specify the nature of the link required between multiple organized armed groups and a party to the conflict in a NIAC in order for them to form a single identifiable party.

Clarifying what constitutes an identifiable party is intricately connected to the intensity requirement. Even if each armed group fulfills the organized armed group criterion, a question remains as to how the intensity requirement is to be met. Specifically, can all of the violence that occurs as

---

103. The membership question is hotly debated. The main disagreement is about which members of an organized armed group may be targeted and when. *See* INTERNATIONAL COMMITTEE OF THE RED CROSS, INTERPRETIVE GUIDANCE ON THE NOTION OF DIRECT PARTICIPATION UNDER INTERNATIONAL HUMANITARIAN LAW 58 (Nils Melzer ed., 2009) [hereinafter ICRC DPH Guidance]. *See also ICRC Clarification Process on the Notion of Direct Participation in Hostilities under International Humanitarian Law (Proceedings)*, INTERNATIONAL COMMITTEE OF THE RED CROSS (June 30, 2009), http://www.icrc.org/eng/resources/documents/article/other/direct-participation-article-020709.htm.

104. *See* ICRC DPH Guidance, *supra* note 103, at 32.

105. Common Article 3 refers to the obligations of "parties" to the conflict, which does not rule out more than one organized armed group. Moreover, the *Commentary* to AP II refers to "insurgents *who are organized in armed groups*," suggesting that multiple armed groups might be a part of the party to the conflict under AP II. AP II COMMENTARY, *supra* note 34, ¶ 4460 (emphasis added).

a result of hostilities with various armed groups be aggregated in order to meet the intensity criterion, or must the level of violence be separately assessed vis-à-vis each armed group? The response to this question may affect whether or not a situation rises to the level of an armed conflict.

The growing acceptance that NIAC law may also apply extraterritorially has brought this issue of links to the forefront in recent years. Although the difficulty arises in internal armed conflicts as well, once territorial constraints are removed from the law's application, it is less obvious that armed groups are part of the same conflict. As a result, the need to ascertain links between these groups increases.

Strictly speaking, it is the hostilities that take place between the specific parties to the conflict that must surpass a level of sporadic violence. It is a well-accepted view that separate conflicts may exist in parallel.[106] Consequently, multiple conflicts may exist side-by-side in the same region. Today many armed groups simultaneously participate in hostilities to varying degrees in a single conflict space. However, in practice, it appears that in some internal NIACs the intensity requirement is not always assessed individually per armed group, but rather through aggregating the violence as a whole. In Iraq, for example, between 2003 and 2009 some estimate that over seventy armed groups existed.[107] Alliances among and between the armed groups frequently shifted,[108] making it difficult to conclude that these armed groups formed a single party to a conflict. Yet, separate assessments were not carried out vis-à-vis each armed group in order to ascertain that the hostilities between specific groups fulfilled the intensity requirement. In reality, the violence conducted by and against each of these groups did not fulfill the criterion of intensity in every case, yet the armed groups were treated as being part of an armed conflict in Iraq.[109] Similar observations can be made with regard to the current conflict in Syria.[110]

---

106. *See, e.g., Tadić* Appeals Decision on Jurisdiction, *supra* note 5, ¶¶ 72−74; ICJ *Nicaragua* Case, *supra* note 36, ¶ 219.

107. *Rule of Law Armed Conflicts Project: Iraq*, GENEVA ACADEMY OF INTERNATIONAL HUMANITARIAN LAW AND HUMAN RIGHTS, http://www.geneva-academy.ch/RULAC/non-state_armed_groups.php?id_state=110 (last visited Feb. 15, 2013). Other armed conflicts, such as those in Syria, the Democratic Republic of Congo, Afghanistan and the former Yugoslavia have involved multiple armed groups.

108. The Mehdi Army for example changed sides a number of times.

109. *See, e.g.,* Michael N. Schmitt, *Iraq (2003 onwards)*, *in* INTERNATIONAL LAW AND THE CLASSIFICATION OF CONFLICTS, *supra* note 25, at 356, 371 ("There is no question but that the fighting in Iraq was sufficiently widespread and intense to meet the violence

Part of the reason for this circumstance could be because it can be difficult to isolate the specific group that conducted each attack and to assign to a particular group some of the indicative factors used to ascertain that the intensity requirement is fulfilled (e.g., determining which group's violence is responsible for fleeing civilians and refugees) given the shared territory. In a way, the common territory serves to link the violence undertaken by these various armed groups.

The question has relevance for characterizing the conflict and targeting. If such an assessment results in the conclusion that a NIAC exists alongside situations of violence that do not reach the threshold of a NIAC (i.e., law enforcement situations), members of the armed group would need to be dealt with through law enforcement means or be treated as civilians directly participating in hostilities.

Not only has there been little emphasis on separating out the intensity of violence generated from each armed group,[111] but also little attention has been given to determining the type of link required to render multiple armed groups part of a single party. This is in notable contrast to the discussion and practice that surrounds the determination of whether parallel IACs and NIACs exist in a country.[112] It is not clear, even for internal

---

threshold or that many of the entities active in the fray amounted to 'organized armed groups.'").

110. The Rule of Law Armed Conflicts Project: Syria identifies the Syrian Free Army as the main armed group, but also lists the following additional armed groups: Syrian branch of the Muslim Brotherhood, Fighting Vanguard, Islamic Liberation Party, Islamic Liberation, Mohammad's Youth, God's Soldiers and Al-Qaeda. *Rule of Law Armed Conflicts Project: Syria,* GENEVA ACADEMY OF INTERNATIONAL HUMANITARIAN LAW AND HUMAN RIGHTS, http://www.geneva-academy.ch/RULAC/non-state_armed_groups.php?id_state=211 (last visited Feb. 15, 2013). More recently, the Syrian Islamic Liberation Front formed as a prominent umbrella organization for Islamist groups. *Syria's Islamist rebels join forces against Assad*, REUTERS, Oct. 11, 2012, *available at* http://www.reuters.com/article/2012/10/11/us-syria-crisis-rebels-idUSBRE89A0Y920121011. For a detailed overview of Islamist groups, see *Holy Warriors: A Field Guide to Syria's Jihadi Groups*, FOREIGN POLICY (Oct. 15, 2012), http://www.foreignpolicy.com/articles/2012/10/15/holy_warriors.

111. Although this practice is by no means uniform. For a list of the separate NIACs occurring in Colombia between the Colombian State and various armed groups and between armed groups, see, e.g., Felicity Szesnat & Annie R. Bird, *Colombia*, *in* INTERNATIONAL LAW AND THE CLASSIFICATION OF CONFLICTS, *supra* note 25, at 203, 227. It should be noted that the distinction made here was between NIACs governed by AP II and those by Common Article 3.

112. For example, the 2011 Libyan conflict could be seen as entailing an IAC between NATO forces and the Libyan government, alongside a NIAC between the Libyan rebels

armed conflicts, if an additional factor must be considered that links armed groups to a party to the conflict in a NIAC.

The questions of what link is required between an organized armed group and a party to the conflict and how the intensity criterion is assessed take on increased significance when applied to an extraterritorial context. In particular, when it comes to a global armed conflict, the lack of clarity has generated disquiet.[113] The United States claims to be in a "global" armed conflict with Al Qaeda and *its affiliates*.[114] The argument is that these affiliated armed groups are connected and collectively constitute a threat to the United States. Therefore, they are part of the same conflict, which happens to be spread out geographically.

However, to simply transfer the model of establishing the requisite level of intensity that is sometimes used in practice in internal (or even regional) armed conflicts to a global armed conflict creates problems. Most importantly, the degree to which these affiliated groups are, in fact, part of the same conflict is less clear in situations spread out across multiple States. Territory no longer serves as a presupposed link between the armed groups that connects the violence. Hostilities undertaken by an affiliated group may be part of an entirely separate conflict. For example, the majority of fighting conducted by groups affiliated with Al Qaeda, such as Al Shabaab in Somalia, often takes place as part of separate internal conflicts.[115] Al Shabaab's interests and targets are predominantly local.[116]

---

and the Libyan government. Likewise, in Afghanistan in 2001, an IAC existed in parallel with a NIAC. *See, e.g.,* Michael N. Schmitt, *Status of Opposition Fighters in a Non-International Armed Conflict*, *in* NON-INTERNATIONAL ARMED CONFLICT IN THE TWENTY-FIRST CENTURY 119 (Kenneth Watkin & Andrew Norris eds., 2012) (Vol. 88, U.S. Naval War College International Law Studies). See Vité for some practical concerns in having a "differentiated approach." Vité, *supra* note 77, at 86.

113. *See, e.g.,* ICRC 2007 Report on IHL and the Challenges of Contemporary Armed Conflict, *supra* note 25, at 725; Pejic*, supra* note 95, at 346; LUBELL, *supra* note 29, at 117; SIVAKUMARAN, *supra* note 30, at 233.

114. *See, e.g.,* John Brennan, Assistant to the President for Homeland Security and Counterterrorism, Remarks at the Center for Strategic and International Studies: **S**ecuring the Homeland by Renewing American Strength, Resilience and Values (May 26, 2010), http://www.whitehouse.gov/the-press-office/remarks-assistant-president-homeland-security-and-counterterrorism-john-brennan-csi [hereinafter Brennan Remarks at CSIS] ("We are at war against al Qaeda and its terrorist affiliates.").

115. *See, e.g.*, Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. on Intelligence, 113th Cong. (2013) (statement of James R. Clapper, Director of National Intelligence, Worldwide Threat Assessment of the US Intelligence Community 4, 5 (Mar. 12, 2013), *available at* http://www.dni.gov/files

At the same time, the law does not specify how multiple organized armed groups might be part of a single party to a conflict in NIACs. Part of the problem is that the test for the existence of an armed conflict has been articulated in terms of the organized armed group requirement in some cases (the *Tadić* test) and at other times in terms of a party to the conflict (Common Article 3). Over the years little attention or clarification has been given to this issue of what constitutes a party to a conflict in NIACs.[117]

The United States claims to be in an armed conflict not only with Al Qaeda, but also with affiliated groups.[118] These affiliates include Al Qaida in the Arabian Peninsula (AQAP), al-Qa'ida in the Islamic Maghreb, Al Shabaab, Al Qaeda in Iraq and Boko Haram (although not formally).[119] Pejic pertinently questions whether the violent acts committed since 9/11 have stemmed from the same group, or if distinct armed groups have carried them out: "[C]an it be said that the totality of terrorist acts that have been perpetrated since 11 September 2011—in Bali, Moscow, Peshawar, Casablanca, Riyadh, Madrid, Istanbul, Beslan, London, Egypt, and elsewhere—constitute a global non-international armed conflict that can be attributed to one and the same party?"[120]

/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf [hereinafter Clapper Statement].

116. *See* Stanford University, *Al-Shabab*, MAPPING MILITANT ORGANIZATIONS, http://www.stanford.edu/group/mappingmilitants/cgi-bin/groups/view/61 (last visited Feb. 15, 2013); NATIONAL COUNTERTERRORISM CENTER, COUNTERTERRORISM 2013 CALENDAR: AL-SHABAB, http://www.nctc.gov/site/groups/al_shabaab.html (Al-Shabab's fighters "are predominantly interested in the nationalistic battle against the TFG [Transitional Federal Government of Somalia] and not supportive of global jihad"). *See, e.g.,* Clapper Statement, *supra* note 115, at 4, 5.

117. *See, e.g.*, Bahia Tahzib-Lie & Olivia Swaak-Goldman, *Determining the Threshold for the Application of International Humanitarian Law, in* MAKING THE VOICE OF HUMANITY HEARD: ESSAYS ON HUMANITARIAN ASSISTANCE AND INTERNATIONAL HUMANITARIAN LAW IN HONOUR OF HRH PRINCESS MARGRIET OF THE NETHERLANDS 248 (Liesbeth Lijnzaad, Johanna Van Sambeek & Bahia Tahzib-Lie eds., 2004) (they point out the importance of the relationship between non-State parties, but do not specify what this relationship might entail).

118. *See, e.g.,* NATIONAL STRATEGY FOR COUNTERTERRORISM, *supra* note 81, at 3; Brennan Remarks at CSIS, *supra* note 114.

119. U.S. DEPARTMENT OF STATE, COUNTRY REPORTS ON TERRORISM 2011: STRATEGIC ASSESSMENT (2012), *available at* http://www.state.gov/j/ct/rls/crt/2011/195540.htm.

120. Pejic, *supra* note 49, at 86, 87. *See also* Kress, *supra* note 14, at 261; SIVAKUMARAN, *supra* note 30, at 233.

Whether these armed groups form a single party to a conflict rests on the degree and type of connection required. Some have suggested that an armed group's declaration of allegiance to the identified party to the conflict (such as was the case with Al Shabaab and Al Qaeda in 2012)[121] suffices for a determination that the affiliated group is part of the same armed conflict. The U.S. government has introduced the terms "associated forces"[122] and "co-belligerents"[123] to describe those armed groups that are affiliated with Al Qaeda and thus part of the global conflict.[124] The meaning and legal basis of these terms are unclear, however. The term "associated" is not found within LOAC. While the concept of "co-belligerency" does surface in international law, it stems from the law of neutrality and pertains only to States.[125] Application of the law of neutrality to hostilities with armed groups is not generally accepted.

---

121. Al Shabaab declared its allegiance to Al Qaeda in February 2012. Bill Rogio, *Somali Islamist Group Formally Declares Allegiance to Shabaab, al Qaeda*, LONG WAR JOURNAL (Feb. 25, 2012), http://www.longwarjournal.org/archives/2012/02/somali_islamist_grou.php.

122. *See, e.g.,* DOJ White Paper *supra* note 1, at 2; NATIONAL STRATEGY FOR COUNTERTERRORISM, *supra* note 81, at 3 n.1 ("*Associated Forces* is a legal term of art that refers to cobelligerents of al-Qa'ida or the Taliban against whom the President is authorized to use force (including the authority to detain) based on the Authorization for the Use of Military Force, Pub. L. 107-40, 115 Stat. 224 (2001)." National Defense Authorization Act for Fiscal Year 2012, Pub. L. 112-81, §1021, 125 Stat.1298, 1562 (2011), *available at* http://www.gpo.gov/fdsys/pkg/PLAW-112publ81/pdf/PLAW-112publ81.pdf (refers to "associated forces that are engaged in hostilities against the United States or its coalition partners."). Although the specification falls under the heading of the authority to detain, statements like the one above indicate that the U.S. government also uses that phrase to signify the parties to the armed conflict in which it is engaged. The United States also refers to "adherents" or "individuals" associated with Al Qaeda. See, for example, the definition provided in the NATIONAL STRATEGY FOR COUNTERTERRORISM, *supra* note 81, at 3.

123. Johnson Oxford Speech, *supra* note 101 ("We have publicly defined an 'associated force' as having two characteristics: (1) an organized, armed group that has entered the fight alongside al Qaeda, and (2) is a co-belligerent with al Qaeda in hostilities against the United States or its coalition partners.").

124. The White House has defined "affiliates" as "[g]roups that have *aligned* with al-Qa'ida." NATIONAL STRATEGY FOR COUNTERTERRORISM, *supra* note 81, at 3 (emphasis added). But it acknowledges in that document that the term is not a legal one. *Id.* at 3 n.1.

125. This was acknowledged in a decision of the U.S. Court of Appeals for the District of Colombia Circuit, which stated:

> [T]he laws of co-belligerency affording notice of war and the choice to remain neutral have only applied to nation states. *See* 2 L. OPPENHEIM, INTERNATIONAL LAW: A TREATISE § 74 (1st ed. 1906). The 55th [Arab Brigade, which included Al Qaeda

Although the law is silent with regard to links between armed groups in NIACs, the concept of links can be found under LOAC for a number of other purposes—namely the criterion of "belonging to a party" used for determining combatant and prisoner of war (POW) status in IACs;[126] the connections necessary to establish a system of responsible command; the two concepts of belligerent nexus used to prove individual criminal responsibility[127] and direct participation in hostilities,[128] respectively; and the link of "overall control" required to internationalize a NIAC.[129] Given the lack of explicit law on the matter, the question examined here is whether any of these existing concepts can be used by analogy for the purpose of determining links between armed groups in a NIAC?

The closest analogy would seem to be to the "belonging to" criterion found under GC III. In order to incorporate an organized armed group into an existing IAC for the purpose of establishing POW and combatancy status, that group must "belong to" a State party to the conflict. At face value, it might seem logical to apply a similar criterion to organized armed groups that are linked to one another in NIACs. A simple transferal of the IAC concept to NIACs, however, is problematic. First, and most importantly, the prerequisite was developed for the specific purpose of establishing qualifications that only exist in international armed conflicts (i.e., POW and combatancy status). Second, the type of link necessary to fulfill the "belonging to" requirement is debated even under IAC law. It is not

---

> members within its command structure] clearly was not a state, but rather an irregular fighting force present within the borders of Afghanistan at the sanction of the Taliban. Any attempt to apply the rules of co-belligerency to such a force would be folly, akin to this court ascribing powers of national sovereignty to a local chapter of the Freemasons.

Al-Bihani v. Obama, 590 F.3d 866, 873 (D.C. Cir. 2010).

126. GC III, *supra* note 4, art. 4(A)(2) ("Members of other militias and members of other volunteer corps, including those of organized resistance movements*, belonging to a Party* to the conflict and operating in or outside their own territory . . . .") (emphasis added); AP I, *supra* note 4, art. 43 ("The armed forces *of a Party* to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates . . . .") (emphasis added).

127. *See, e.g., Kunarac* Appeals Judgment, *supra* note 52, ¶ 58; Prosecutor v. Rutaganda, Case No. ICTR-96–3, Appeals Chamber Judgment, ¶ 570 (May 26, 2003).

128. ICRC DPH Guidance, *supra* note 103, at 58.

129. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Judgment, ¶¶ 122, 156 (Int'l Crim. Trib. for the former Yugoslavia July 15, 1999) [hereinafter *Tadić* Appeals Judgment].

clear whether the criterion calls for a link of control or coordination.[130] Thus, transferring the concept to NIACs will not likely provide greater clarity.

The ICRC's *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* does introduce the idea that an organized armed group may "belong to" a party to the conflict in a NIAC.[131] The *Guidance*'s interpretation of the concept is taken from the third Geneva Convention and corresponds with those who consider that a link of coordination suffices (as opposed to control).[132] There are, however, several concerns in relying on the *Guidance*'s articulation of "belonging to" in NIACs. Most importantly, the *Guidance* does not provide a legal basis for the inclusion of this criterion in NIACs. Rather, it extends the meaning of "belonging to" established for the purpose of determining POW and combatancy status in IACs to a NIAC context, where such status does not exist.[133] Moreover, the *Guidance* seems to conflate the vernacular use for whether an individual belongs to an armed group, with the legal notion de-

130. For the interpretations that tend to view the link as one of coordination, see, e.g., GC III COMMENTARY, *supra* note 5, at 57 (Article 4); Michael N. Schmitt *Humanitarian Law and Direct Participation in Hostilities by Private Contractors or Civilian Employees*, 5 CHICAGO JOURNAL OF INTERNATIONAL LAW 528 (2005). Examples of those who view the link as one of control are Hays Parks, *Combatants*, *in* THE WAR IN AFGHANISTAN: A LEGAL ANALYSIS 247, 269 (Michael N. Schmitt ed., 2012) (Vol. 85, U.S. Naval War College International Law Studies) and the Israeli Military Court in *Military Prosecutor* v. *Kassem* (Israeli Military Court, Apr. 13, 1971), *reprinted in* 42 INTERNATIONAL LAW REPORTS 476, 477 (1971).

131. ICRC DPH Guidance, *supra* note 103, at 31 ("Organized armed groups *belonging to* a non-State party to an armed conflict include both dissident armed forces and other organized armed groups.") (emphasis added). While the *Guidance*'s discussion focuses on targeting, its proposal leaves room for the interpretation that multiple armed groups could be linked to one party in a NIAC. It should be noted the *Guidance* does not constitute law. However, it may influence the way in which the law develops.

132. The *Guidance* requires that there is "at least a de facto relationship between an organized armed group and a party to the conflict" and considers that "conclusive behaviour that makes clear for which party the group is fighting" wo*uld suffice*. *Id.* at 23. The *Guidance* takes this definition directly from the ICRC *Commentary* to the Third Geneva Convention. GC III COMMENTARY, *supra* note 5, at 57 (Article 4).

133. In addition, the same criticism that the *Guidance* has received for requiring that an organized armed group belong to a party to an IAC applies in the case of NIACs. Some consider it problematic to use a criterion that exists for the purposes of detention in order to determine who may be targeted. *See, e.g.*, Michael N. Schmitt, *The Interpretive Guidance: A Critical Analysis*, 1 HARVARD NATIONAL SECURITY JOURNAL 18 (2009). It should also be noted that the *Guidance* discusses the criterion in the context of targeting, rather than for the purposes of establishing the existence of an armed conflict.

veloped under the law of armed conflict for whether or not an armed group "belongs to" a party to an IAC.[134] Given these factors, employing the "belonging to" link by analogy may lead to further complication, rather than clarifying the circumstances for when organized armed groups may be linked to one another for the purpose of establishing when an armed conflict exists.

Another reasonable analogy might be to require that the organized armed group falls under a responsible command of a party to the conflict. If the affiliated group were required to be under the responsible command of the party to the conflict, a stronger link would be necessary than, for example, simply sharing a common ideology with, or being inspired by, Al Qaeda.[135] In the case of groups affiliated with Al Qaeda, the fact that armed groups pledge allegiance or change their name does not mean they become part of Al Qaeda's command structure.[136] Accordingly, some of the groups affiliated with Al Qaeda would not form part of a single identifiable party to the conflict under this interpretation. They could still be parties to separate armed conflicts if the intensity criterion was fulfilled. A benefit of turning to responsible command for establishing the link is that the concept already exists in NIAC law.[137] The difficulty is that being part of a responsible command would likely necessitate a high threshold of control. For instance, the link required by a responsible command would likely not encompass organized armed groups that act in a coordinated manner, a circumstance that frequently occurs today.

An analogy to a belligerent nexus also raises concerns. Most significantly, the concepts of belligerent nexus currently found in the law (both as used to establish individual criminal responsibility and as a constitutive element of direct participation in hostilities) pertain to the relationship between the acts of an individual and an armed conflict. Such a relationship

---

134. For example, the COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 34, ¶ 4789, uses the term "belonging to" with reference to membership into a group in a NIAC ("[t]hose who *belong to* armed forces or armed groups may be attacked at any time") (emphasis added).

135. *See, e.g.,* ICRC 2007 Report on IHL and the Challenges of Contemporary Armed Conflict, *supra* note 25, at 725; Pejic, *supra* note 95, at 346; LUBELL, *supra* note 29, at 117, 118; SIVAKUMARAN, *supra* note 30, at 233.

136. DANIEL L. BYMAN, BREAKING THE BONDS BETWEEN AL-QAIDA AND ITS AFFILIATE ORGANIZATIONS 11 (2012), *available at* http://www.brookings.edu/~/media/research/files/papers/2012/7/alqaida%20terrorism%20byman/alqaida%20terrorism%20byman.pdf.

137. AP II, *supra* note 6, art. 1.

must be distinguished from linking the actions of an armed group to those of another armed group or a party to the conflict. Therefore, the concept does not correspond directly to the issue under discussion.[138]

The "overall control" test used to internationalize a non-international armed conflict could also provide a template. As articulated in the ICTY's *Tadić* appeals judgment, the State party to a conflict need not direct specific actions, but must have overall control of the armed group in question.[139] This test requires a high standard of control over an armed group as it is developed for the purpose of triggering the full body of IAC law. The purpose of the test would be different in the NIAC context—to link an armed group to a party to a NIAC with consequences for targeting. It is, therefore, not self-evident that the same test would be appropriate. Moreover, if transferred to NIACs, this test would necessitate that one armed group party to the conflict have overall control of another armed group. Today this often is not the case.

In sum, these analogies are not particularly helpful in addressing the challenge presented by multiple organized armed groups connected to varying degrees to one another and to a party to the conflict. Given the lack of clarity in the law concerning identifiable parties, the question remains whether the armed groups can still be part of the same conflict, such that their hostilities are accumulated in order to establish the requisite level of intensity for an armed conflict to exist.

One option is to apply the intensity test more strictly in situations of global armed conflicts, assessing the requirement solely based on the violence that occurs between the specific parties to that conflict. Any violence with affiliated armed groups would be considered separately. As a consequence, some situations might not fulfill the intensity requirement and, therefore, not qualify as an armed conflict (either because the situation as a

138. Interestingly, one of the key authors of the ICRC *Guidance*, Nils Melzer, equates this "belonging to" link to that of a belligerent nexus. Melzer states that for an armed group even to be part of an IAC the violence conducted by that armed group must be "designed to support one of the belligerents against another (belligerent nexus)." Nils Melzer, *Keeping the Balance between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities*, 42 NEW YORK UNIVERSITY JOURNAL OF INTERNATIONAL LAW AND POLITICS 831, 841 (2010). He continues, "[w]hether or not a group is involved in hostilities does not only depend on whether it resorts to organized armed violence temporally and geographically coinciding with a situation of armed conflict, but also on whether such violence is designed to support one of the belligerents against another (belligerent nexus)." *Id.*

139. *Tadić* Appeals Judgment, *supra* note 129, ¶ 122.

whole does not fulfill the intensity requirement or because a particular circumstance is not considered to be part of an existing armed conflict).[140] A law enforcement regime then would apply, affecting the applicable rules on targeting and detention.

However, this approach does not deal with the realities of some conflicts today where armed groups may be linked with one another to differing degrees and over geographic distances. As a consequence, States may reject this option on the ground that it does not provide adequate means to address what they view as a threat. Furthermore, in situations where separate ongoing internal conflicts take place—such as in Somalia—the normal law enforcement regime may not be wholly functional. This absence, along with the outside State's inability to legally resort to the law of armed conflict, could result in a legal gap. Considering that one of the initial underlying reasons for developing NIAC law was prevention of a legal black hole, such an outcome is not optimal.

An alternative suggestion is to develop an additional requirement—that the affiliated armed group constitute a *threat* to the State party. The term "threat" here refers to an actual threat based on the intentions and actions of the armed group. In a sense, this extra condition suggests that the purpose of the group would matter.[141] The purpose here does not refer to a political purpose, but that the armed group's main purpose, as evidenced by its actions, is fighting the State in question. An assessment of who the group targets and what their goals are would indicate whether the armed group was a threat and thus actually part of the global conflict. As a consequence, violence stemming from armed conflicts that are separate from the threat posed to the State could not be factored into the same intensity assessment.

So, for example, a number of different armed groups participate in the hostilities in Yemen. Fighting is taking place in the north between the Al-Houthi tribe and the Yemeni government; in the south with Southern Mobility Movement attempting to secede;[142] and throughout the country be-

140. A State could still be involved in an armed conflict if invited by the territorial State. For example, the United States could legitimately be part of the armed conflict against AQAP in Yemen, after being asked to fight on behalf of the Yemeni government. However, this would not constitute a "global" armed conflict.

141. Currently, the majority view is that the purpose of an armed group does not matter when determining if an armed conflict exists. *See, e.g.,* 31st ICRC Conference on IHL CHALLENGES*, supra* note 15, at 11; Vité, *supra* note 77, at 78.

142. *Armed Conflict Database: Yemen (Houthis/AQAP/SMM)*, INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES, https://acd.iiss.org/en/conflicts/yemen--houthis-aqap-

tween AQAP and the Yemeni government.[143] Even if AQAP is considered to be part of Al Qaeda, the violence taking place in Yemen relating to the internal conflict could not be factored into the intensity assessment in the U.S. conflict against Al Qaeda and its affiliates. Put differently, because the hostilities of these other armed groups are not directed against the United States, they are not part of the same conflict.

This suggestion addresses the lack of clarity in what constitutes the identifiable party to the conflict when conflicts become more geographically dispersed and multiple organized armed groups are involved. It also serves to place a constraint on when and where an armed conflict may exist. At the same time, it has the benefit of maintaining consistency with internal conflicts.

There are clear risks, however, in considering that the purpose of an armed group might matter. Most notably, the subjective nature of determining a purpose, particularly in an environment where the same group may have multiple agendas, poses practical challenges. Moreover, just as it may be difficult to separate out the hostilities conducted by multiple armed groups for the purpose of establishing the intensity requirement in internal conflicts, the same issue easily arises with hostilities that span multiple territories. Finally, this suggestion of looking to the threat posed by the armed group does not reflect current law.

The point here is that the issue of links between organized armed groups and the calculation of the intensity requirement is an area where the law needs more clarity, particularly in a global context.

C. Intensity Criterion and Conglomeration of Violence over Space

Even if the various affiliated groups are considered to be involved in a single conflict, a second issue arises as to how the intensity requirement should be assessed in global conflict. Does the distribution of violence over multiple territories make the hostilities less intense? Put differently, if the overall level of violence was deemed sufficiently intense to satisfy the *Tadić*

---

smm-9651 (last visited Aug. 2, 2013); BYMAN, *supra* note 136, at 11 ("Even AQAP, often touted as the affiliate closest to al-Qa'ida because it has attempted attacks on American civil aviation—perhaps the ultimate target for the al-Qa'ida core—still concentrates primarily on targets within Yemen itself.").

143. *Rule of Law Armed Conflicts Project: Yemen*, GENEVA ACADEMY OF INTERNATIONAL HUMANITARIAN LAW AND HUMAN RIGHTS, http://www.geneva-academy.ch/RULAC/current_conflict.php?id_state=234 (last visited Feb. 15, 2013).

test, should it matter whether that violence occurred entirely within a single State or was instead spread over multiple States, such that in each State it is sporadic?

Given the lack of clarity on the matter, it is useful to resort to the underlying purpose of the intensity requirement. The criterion is intended to differentiate a situation of armed conflict from one of internal disturbances, or as articulated by ICTY case law, "to distinguish an armed conflict from banditry, unorganized and short-lived insurrections, or terrorist activities, all of which are not subject to international law."[144] The law does not define internal disturbances. ICRC internal guidance, however, on the meaning of the phrase states that internal disturbances can range from "the spontaneous generation of acts of revolt to the struggle between more or less organized groups and the authorities in power. In these situations, which do not necessarily degenerate into open struggle, the authorities in power call upon extensive police forces, or even armed forces, to restore internal order."[145] As discussed earlier, the intensity requirement includes both components of gravity and duration.[146] The question here revolves around whether the geographic diffusion of violence renders it less grave.

An underlying purpose of the intensity requirement was to differentiate between situations where the normal domestic law regime of the country in conflict would be sufficient to deal with the unrest and those where a break-down in the system occurred.[147] In the case of a global armed conflict where the violence is spread out geographically, if the necessary level of intensity (in terms of gravity) is not present in each territory then arguably there may not be a basis upon which to resort to a LOAC regime. In such a case, presumably normal domestic law and human rights regimes

---

144. *Milosević* Decision, *supra* note 52, ¶ 26. *See also Tadić* Trial Judgment, *supra* note 51, ¶ 562; *Delalić* Trial Judgment, *supra* note 51, ¶ 184; *Limaj* Trial Judgment, *supra* note 32, ¶ 84; Corrected Letter of January 28, 1998 from Christopher Hulse, Ambassador of the United Kingdom, to the Swiss Government (July 2, 2002), *available at* http://www.icrc.org/ihl/NORM/0A9E03F0F2EE757CC1256402003FB6D2?OpenDocument (setting forth the UK government's reservation to Article 1(4) of AP I). Note: the designation of a group or acts by a group as "terrorist" has no bearing on whether LOAC applies. Either the acts/situation amounts to one of armed conflict or it does not. *See, e.g.*, *Djordjević* Trial Judgment, *supra* note 57, ¶ 1524, citing the *Boškoski* Trial Judgment, *supra* note 52, ¶ 5763.

145. COMMENTARY ON THE ADDITIONAL PROTOCOLS, *supra* note 34, ¶ 4475. *See also id.*, ¶¶ 4474–77.

146. *See supra* notes 65, 66 and accompanying text.

147. *See, e.g.*, *Tadić* Trial Judgment, *supra* note 51, ¶ 562; Geiss, *supra* note 39, at 138. Domestic law continues to apply in situations of armed conflict.

would be sufficient to deal with the matter.[148] A counterargument to this perspective is that, from the point of view of the parties to the conflict, the consequences are the same whether the violence emanates from one territory or several. However, the intensity requirement has not been determined in the past by the effects on the opposing party alone. The calculation of the intensity requirement has generally included an assessment of the situation as a whole. Factors such as civilians fleeing the conflict zone, occupation of territory, existence of front lines and quantity of troops deployed have been considered.[149] These elements indicate that the violence is linked, at least to a geographic region, if not with a State. Therefore, when hostilities are so dispersed that the domestic legal regime is able to function, it could be difficult to maintain that an armed conflict exists.

D. Intensity Criterion and State Sovereignty

State sovereignty was another impetus for creating the requirement that the hostilities reach a certain level of intensity before LOAC could apply. States wanted to limit the involvement of outside States in their domestic affairs. This objective must, therefore, be seen in light of the fact that the types of conflicts envisioned were mainly internal armed conflicts. In an extraterritorial NIAC context, the reluctance of the State party to the conflict to be subject to interference from other States in its internal affairs largely disappears.[150] Neither internal disturbances nor the conflict itself takes place in their own territory.

Does it matter in terms of what LOAC requires for its application that it is the State *not* party to the conflict whose territorial integrity is infringed? In other words, could this geographic shift in where the hostilities occur affect one of the original underlying reasons for the existence of the threshold? In contrast to the previous two points (whether the violence undertaken by various armed groups may be conglomerated and whether the distribution of violence over space means that it does not reach the sufficient level of intensity), this point questions whether the level of intensity

148. The separate issue then would arise of how one State may exercise law enforcement authority in a second State without violating its sovereignty.

149. *Boškoski* Trial Judgment, *supra* note 52, ¶ 177. *See, e.g.,* Louise Arimatsu, *The Democratic Republic of the Congo 1993–2012*, *in* INTERNATIONAL LAW AND THE CLASSIFICATION OF CONFLICTS, *supra* note 25, at 146, 153.

150. *See* Sassòli, *supra* note 30.

customarily required for internal armed conflicts is the same for extraterritorial conflicts.

It may be argued that the territorial State (i.e., the State in which an extraterritorial NIAC physically takes place) has an interest in trying to prevent incursions into its sovereignty, even though it may not be a party to that NIAC. An incursion by an outside State in order to fight an armed group would likely have implications for the "uninvolved" territorial State. For instance, such an action could be an indication that the territorial State is not able to maintain its own security—an image that States usually take pains to avoid. Or, the territorial State may be concerned that the outside State might gain control or influence within their State.

The implications this shift might have on establishing the threshold of an extraterritorial armed conflict are not clear. At the very least, the reassignment of which State's sovereignty is affected indicates that issues arising from the shifted location of the conflict warrant further examination. Therefore, even if one accepts the premise that NIACs may exist extraterritorially, the fact that the law was designed for a different context presents challenges in determining the existence of an armed conflict.

VI. GEOGRAPHIC BOUNDARIES OF EXISTING ARMED CONFLICTS

The removal of territorial boundaries from a system based on these physical limits raises the related question of *where* LOAC may be applied once the law of armed conflict has been triggered. Limited discussion has arisen previously on this issue in the context of purely internal conflicts. However, the main controversy surfaces today specifically with regard to individuals affiliated with an organized armed group located in a second State ("outside of an active battlefield"[151]). The unease of some commentators that the world could become a battlefield reappears here.

Because NIAC law was designed for internal application, its extraterritorial parameters are not clear. Two main options have been discussed for how to deal with this challenge. One proposes that the geographic application of LOAC is limited to the area of hostilities. The other maintains that

151. John Brennan, Assistant to the President for Homeland Security and Counterterrorism Remarks at Woodrow Wilson International Center for Scholars: The Ethics and Efficacy of the President's Counterterrorism Strategy (Apr. 30, 2012), *available at* http://www.cfr.org/counterterrorism/brennans-speech-counterterrorism-april-2012/p28100 [hereinafter Brennan Speech at the Woodrow Wilson Center]. *See also* DOJ White Paper, *supra* note 1.

once an armed conflict exists the law may extend beyond the immediate zone of hostilities. This latter approach has been interpreted by some to suggest that the law applies to the parties to the conflict wherever they may be located.

The first proposal, suggesting that LOAC would not apply at a distance from wherever the hostilities were taking place,[152] may seem logical on its face, but lacks a legal basis. Jurisprudence from the ICTY dealing with the geographic scope of Common Article 3 *within* a State contradicts this interpretation, providing that "international humanitarian law continues to apply . . . in the case of internal conflicts . . . [to] the whole territory under the control of a party, whether or not actual combat takes place there."[153] The ICTY case law has generally been interpreted by other bodies to mean that Common Article 3 applies to the entire country in which a conflict is taking place, regardless of where hostilities occur.[154] This language has been repeatedly upheld by subsequent ICTY and ICTR judgments.[155] In the absence of explicit treaty law or customary international law, this jurisprudence could be said to have relevance when it comes to interpreting the geographic contours of internal conflicts.

Resort to the object and purpose of the law also supports application of the law beyond areas of hostilities. One of the law's fundamental purposes is to ensure protection of individuals once in the hands of the enemy. To interpret the law as only applying to areas of combat would reduce

---

152. Jennifer Daskal, for example, discusses the "hot" battlefield. Jennifer C. Daskal *The Geography of the Battlefield: A Framework for Detention and Targeting Outside the "Hot" Conflict Zone*, 161 UNIVERSITY OF PENNSYLVANIA LAW REVIEW 1165, 1192–1209 (2013).

153. *Tadić* Appeals Decision on Jurisdiction, *supra* note 5, ¶ 70.

154. *See, e.g., Akayesu* Trial Judgment, *supra* note 34, ¶¶ 635−36; Prosecutor v. Kayishema, Case No. ICTR-95-1-T, Trial Judgment, ¶176 (May 29, 1999); GS (Existence of internal armed conflict) Afghanistan [2009] UKAIT 00010 (U.K. Asylum and Immigration Tribunal); Economic and Social Council, Commission on Human Rights, Report of the Independent Expert, *Situation of Human Rights in Somalia*, ¶ 31, U.N. Doc. E/CN.4/2002/119 (Jan. 14, 2002) (by Ghanim Alnajjar). *See also* Kress, *supra* note 14, at 265.

155. *See, e.g., Blaskić* Trial Judgment, *supra* note 39, ¶ 64; *Delalić* Trial Judgment, *supra* note 51, ¶¶ 185, 194, 209; Prosecutor v. Aleksovski, Case No. IT-95-14/1-T, Judgment, ¶ 43 (Int'l Crim. Trib. for the former Yugoslavia June 25, 1999); Prosecutor v. Kunarac, Case No. IT-96-23-T & IT-96-23/1-T, Judgment, ¶ 568 (Int'l Crim. Trib. for the former Yugoslavia Feb. 22, 2001); *Kunarac* Appeals Judgment, *supra* note, 52, ¶ 57; *Limaj* Trial Judgment, *supra* note 32, ¶ 84, Kordić and Čerkez, Case No. IT-95-14/2-T, Judgment, ¶ 27 (Int'l Crim. Trib. for the former Yugoslavia Feb. 26, 2001).

the protection afforded to some of the most vulnerable, who may be located at a distance from active hostilities.

Finally, the text of AP II can be turned to for some guidance, even though the types of conflicts under discussion here are those with a lower threshold. AP II explicitly provides that it applies to "to all persons affected by an armed conflict."[156] This indicates that although AP II limits its applicability to the State in which the conflict is taking place,[157] its application is not restricted to areas of active hostilities.[158]

The second approach considers that once an armed conflict exists LOAC applies beyond the area of active hostilities.[159] It is argued that this is the more defensible position of the two. Although this view does not find an explicit basis in treaty law, it is difficult to find justification within the existing law for restricting the application of LOAC to a certain region once an armed conflict exists. In addition, the ICTY and ICTR case law just noted could be said to indirectly support this position in that it interprets the application of the law as extending beyond the combat zones. However, too much reliance on this jurisprudence is misguided as it still depends on State boundaries. For example, if one accepts that the armed conflict in Afghanistan has spilled over into Pakistan, does Common Article 3 then apply throughout the country of Pakistan?

The view that LOAC applies beyond the area of active hostilities leads to the question of whether anything restricts the geographic application of LOAC. One approach is to interpret the ICTY case law as literally referring to the areas where the parties to the conflict have control.[160] Under

---

156. Art. 2 AP II. *See also* arts. 5, 6 AP II and Noam Lubell & Nathan Derejko, *A Global Battlefield: Drones and the Geographical Scope of Armed Conflict*, 11 JOURNAL OF INTERNATIONAL CRIMINAL JUSTICE 65, 75-76 (2013).

157. While there has been discussion that Common Article 3 applies extraterritorially, there has been very little debate regarding AP II's extraterritorial reach.

158. The ICRC *Commentary* to AP II supports this interpretation. AP II COMMENTARY, *supra* note 34, ¶ 4490 ("[p]ersons affected by the conflict within the meaning of this paragraph are covered by the Protocol *wherever they are in the territory* of the State engaged in conflict" and that the "applicability of protocol follows from a criteria related to persons, and not to places") (emphasis added).

159. *See, e.g.,* Lubell & Derejko, *supra* note 156, at 82. (". . . the applicability of the *ius in* bello does not depend on the number of miles between the individual and the fighters they are commanding and directing, nor does it stand or fall on whether the individual is sitting on one side of a border or another. The tests are the standard and long-recognized requirements for determining who or what is a legitimate target under IHL . . . .")

160. Kress proposes a version of this interpretation by suggesting that the law extends only to areas where "the non-State party has established an actual (quasi-) military infra-

such a view, NIAC law would only apply to the territory under control of the Pakistani Taliban (and other armed groups) in the North-West Frontier Province. This construction, however, presents hurdles.[161] First, what is meant by control?[162] Second, if it is territorial control that is envisioned, the majority of commentators and jurisprudence view the control of territory by an armed group as an indicator for the applicability of Common Article 3, rather than an obligation.[163] It would not make sense to require territorial control by an armed group in order to determine the reach of an armed conflict within a country, but not to require territorial control for the existence of an armed conflict.[164] Third, taken to its extreme this interpretation illogically suggests that if neither party controls territory, then LOAC does not apply,[165] leading to the possibility that LOAC would not apply precisely where the battle rages.

The U.S. government position that LOAC is not geographically constrained with regard to individual members of a party to a conflict[166] has engendered criticism.[167] However, it is a defensible stance if one has already accepted that the territorial boundaries of States do not limit LOAC's application. The bigger issue seems to be that the law was not designed for extraterritorial application. As such, should the view that territorial boundaries are not relevant to LOAC's application gain force, it may be that the law will develop in a clearer and more nuanced manner.[168]

---

structure on the territory of the third State's soil that would enable the non-State party to carry out intensive armed violence also from there". Kress, *supra* note 14, at 266.

161. *See, e.g.,* Arimatsu, *supra* note 2, at 187, 188.

162. Arimatsu points this out in *id.* at 188.

163. *See, e.g.*, PROVOST, *supra* note 46, at 267; MOIR, *supra* note 41, at 38, 43; Pejic, *supra* note 82, at 85−86; BOTHE, *supra* note 62, at 623; Tahzib-Lie & Swaak-Goldman, *supra* note 117, at 246; Vité, *supra* note 77, at 79.

164. Lubell & Derejko, *supra* note 156, at 69.

165. *Id.* However, Kress's suggestion that there must be actual military infrastructure with the ability to carry out intensive violence avoids the issue of control. Kress, *supra* note 14, at 266.

166. *See, e.g.,* Brennan Speech at the Woodrow Wilson Center, *supra* note 151 ("There is nothing in international law that . . . prohibits us from using lethal force against our enemies outside of an active battlefield, at least when the country involved consents or is unable or unwilling to take action against the threat.")

167. Kress, *supra* note 14, at 266.

168. Interestingly, while of the view that the law follows the parties to the conflict, the U.S. government places additional policy restraints onto the application of LOAC. The DOJ White Paper states that when targeting an individual located in another country in the context of an extraterritorial NIAC, the individual must be high ranking in the organization, the armed group should have a "significant and organized presence" in that coun-

Notwithstanding the lack of clarity with regard to this issue, significant restrictions on the use of force against an individual located at a distance from hostilities in a second country already exist. Perhaps most importantly, the question only arises in the first place if an armed conflict exists between the State using force and the armed group against which the force is directed (which includes establishing that the group to which the individual belongs is an identifiable party). Second, and crucially, the separate question then arises of whether an individual is targetable (either by virtue of the membership approach or because s/he is directly participating in hostilities).[169] This includes determining that the individual in question has a sufficient nexus to the ongoing armed conflict.[170]

Should those conditions be fulfilled, then the constraints within LOAC still apply (such as all of the rules pertaining to the principles of distinction and proportionality), as would the country's domestic law and human rights law to the degree that it interacts with LOAC. It is likely that if the occurrence were far from active hostilities the latter two bodies of law would play a greater role. Issues of State sovereignty could, and often do, present one of the greatest limitations on action. Therefore, it is not the case that force may be used anywhere in the world at any time against parties to the conflict once an armed conflict exists.

VII. CONCLUSION

In conclusion, the general trend today is that some extraterritorial conflicts may qualify as NIACs, despite the fact that they are not geographically confined to a single State. This interpretation recognizes that to artificially re-

try and the location should be one from which "senior operational leaders, plan attacks against U.S. persons and interests." DOJ White Paper, *supra* note 1, at 3, 5 ("The United States retains its authority to use force against al-Qa'eda and associated forces outside the area of active hostilities when it targets a senior operational leader of the enemy forces who is actively engaged in planning operations to kill Americans." "If an operation . . . were to occur in a location where al-Qa'ida or an associated force has a significant and organized presence and from which al-Qa'ida or an associated force, including its senior operational leaders, plan attacks against U.S. persons and interests, the operation would be part of the non-international armed conflict between the United States and al-Qa'ida that the Supreme Court recognized in *Hamdan*."). Although the leaked memorandum is in specific reference to American citizens, this statement seems to refer more generally to the scope of non-international armed conflict.

169. See *supra* note 103 for reference to the debate on membership.

170. Lubell & Derejko, *supra* note 156, at 75.

strict the law in a way that does not reflect either the realities on the ground or the purpose of the law itself is counterproductive. However, because the existing law was not designed for extraterritorial conflicts, challenges arise in its application.

The issue of links between armed groups in NIACs is an area where the law may need reinterpretation or development. Analogies with other areas of the law do not lead to more clarity. The tenuous suggestion that in order to fulfill the intensity requirement not only should the affiliated armed group be organized and part of an identifiable party, but also that the group's actions and goals should constitute a threat to the opposing party carries with it practical problems. Specifically, it could be difficult to ascertain both the threat and which members of an armed group are actually participating in actions that are part of the global conflict, as opposed to part of a separate internal conflict.

Determining whether amassing violence that is diffused over distances may fulfill the intensity requirement is another example of how the geographic extension of the law's application may present difficulties. It has been argued here that taking into account the underlying purpose of the law, the violence must reach a certain level of intensity within a geographic region for an armed conflict to exist. When the violence is spread out geographically, such that in an individual country the law enforcement regimes may function, it is difficult to view the intensity requirement as being met. However, as with links, this issue is far from resolved.

The third principal challenge resulting from the extraterritorial application of NIAC law is that a reassignment of sovereignty occurs. It is unclear if this shift might impact on how States perceive the threshold of the existence of an armed conflict.

Once the existence of an armed conflict has been established, a separate issue arises as to the geographic boundaries of that conflict. This impacts the controversial question of when an individual may be targeted or detained if located in another country away from the main battlefield. Here too, because the law was originally intended to apply within State boundaries, very little guidance exists. It is argued that as the law currently stands, once an armed conflict exists LOAC applies to the parties to the conflict wherever they may be located, but that other restraints within LOAC and *jus ad bellum* limit its application. In particular, the question of whether an armed conflict exists in the first place is not self-evident. The debate on who can be targeted and when applies both to internal NIACs and extraterritorial NIACs. It may be that additional stipulations will be considered

necessary as the law develops given the lack of State boundaries and the distance from an active battlefield. However, currently the law does not require this. Finally, the restrictions found in *jus ad bellum* curtail action that may be taken.

Therefore, to erase territorial boundaries from the equation entirely when establishing the existence of an armed conflict raises challenges to the structure of the law and some of its underlying purposes. Certain obstacles may prompt clarification in the law; others may remain as limitations on the law's application. As a consequence, it is not clear where the bar for the application of Common Article 3, and thus LOAC, lies, particularly when applied to conflicts that spread across multiple countries. Some States want to ensure that they have sufficient flexibility to deal with these circumstances. Other States (as well as organizations and commentators) are concerned that the law may be interpreted too permissively and ultimately be abused. A balance must be found in the solution to these issues.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

The Syrian Intervention: Assessing the Possible International Law Justifications

Michael N. Schmitt

89 INT'L L. STUD. 744 (2013)

Volume 89 2013

The Syrian Intervention: Assessing the Possible International Law Justifications

Michael N. Schmitt[*]

I. INTRODUCTION

The seemingly tangential nature of international law to the debate regarding strikes on Syria is both remarkable and disheartening.[1] With war clouds looming, the Administration has yet to fully present its legal justification for military action. Instead, President Obama has merely signaled his willingness to go "forward without the approval of a United Nations Security Council that, so far, has been completely paralyzed and unwilling to hold

* Stockton Professor and Chairman, International Law Department, United States Naval War College; Professor of Public International Law, University of Exeter. The views expressed in this article are those of the author in his personal capacity and do not necessarily represent those of the United States government.

1. The U.S. operations would be in response to alleged, repeated use by the Assad regime of chemical weapons. On the chemical attacks, see Chairman, United Kingdom Joint Intelligence Committee, Syria: Reporting Chemical Weapons Use, Aug. 29, 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/235094/Jp_115_JD_PM_Syria_Reported_Chemical_Weapon_Use_with_annex.pdf. The most significant event occurred on August, 21, 2013. U.S. estimates are that over 1000 people died in that attack, whereas the British estimate is approximately 350. Contrast The White House, Statement by the President on Syria, Aug. 31, 2013, http://www.whitehouse.gov/the-press-office/2013/08/31/statement-president-syria, with Joint Intelligence Organisation, Assessment on Reported Chemical Weapons Use in Damascus, Aug. 27, 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/235094/Jp_115_JD_PM_Syria_Reported_Chemical_Weapon_Use_with_annex.pdf.

Assad accountable." He explains that the most recent and severe chemical weapons attack on 21 August 2013

> . . . is an assault on human dignity. It also presents a serious danger to our national security. It risks making a mockery of the global prohibition on the use of chemical weapons. It endangers our friends and our partners along Syria's borders, including Israel, Jordan, Turkey, Lebanon and Iraq. It could lead to escalating use of chemical weapons, or their proliferation to terrorist groups who would do our people harm.[2]

Use of armed force by one State against another has two legal consequences. First, military operations at the level currently contemplated with respect to Syria initiate an "international armed conflict" in which the *jus in bello* (international humanitarian law) governs how the ensuing hostilities may be conducted.[3] The objectives of the attacking State are irrelevant to the existence of an armed conflict, which is an entirely fact-based legal status. Similarly, although disagreement exists over whether low levels of violence qualify as armed conflict,[4] there is no question that operations involving cruise missiles or other aerial strikes reach this threshold.[5] In lay terms, the launch of military operations by the United States and its partners against Syria would mean those countries were "at war" as a matter of international law.

Second, the resort to military force by a State constitutes a "use of force" under the *jus ad bellum*. The *jus ad bellum* addresses the issue of when

---

2. Statement by the President, *supra* note 1.

3. Prosecutor v. Tadić, Case No. IT-94-1-I, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia, Oct. 2, 1995).

4. *See, e.g.*, Christopher Greenwood, *Scope of Application of Humanitarian Law*, in THE HANDBOOK OF INTERNATIONAL HUMANITARIAN LAW 45, 57 (Dieter Fleck ed., 2d ed. 2008).

5. "Any difference arising between two States and leading to the intervention of armed forces is an armed conflict [qualifies as an armed conflict] . . . . It makes no difference how long the conflict lasts or how much slaughter takes place." COMMENTARY: GENEVA CONVENTION FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED AND SICK IN ARMED FORCES IN THE FIELD 32 (Jean Pictet ed., 1952); COMMENTARY: GENEVA CONVENTION FOR THE AMELIORATION OF THE CONDITION OF THE WOUNDED, SICK AND SHIPWRECKED MEMBERS OF THE ARMED FORCES AT SEA 28 (Jean Pictet ed., 1960); COMMENTARY: GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR OF AUGUST 12, 1949 23 (Jean Pictet ed., 1960); COMMENTARY: GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIME OF WAR 20 (Jean Pictet ed., 1958).

States may use force as an instrument of their national policies. Its most fundamental norm is the prohibition found in customary law and set forth in Article 2(4) of the U.N. Charter: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."[6] Absent an applicable exception to this proscription, U.S. military operations against Syria will arguably violate international law.

This inaugural contribution to the "Current Developments" section of *International Law Studies* explores the possible legal justifications for using armed force against Syria. The analysis draws solely on international law; no effort is made to examine Presidential authority to order strikes under U.S. law. The article concludes that there is no unassailable legal basis for the operations. Therefore, it is imperative that the Administration provide its legal justification in order to inform the ongoing debate and before ordering U.S. forces into harm's way.

II. POSSIBLE LEGAL JUSTIFICATIONS

A. Security Council Authorization

The U.N. Charter contains two express exceptions to the prohibition on the use of force.[7] Security Council authorization pursuant to Articles 39 and 42 is the first. By those articles, the Council is authorized to "determine the existence of any threat to the peace, breach of the peace, or act of aggression" and decide upon measures, including the use of force, necessary "to maintain or restore international peace and security." There is no question that a Security Council Resolution authorizing "all necessary means" (U.N. shorthand for "force") to respond to Syria's use of chemical weapons, or to more broadly address the humanitarian disaster in the country, would be lawful. Indeed, the Security Council has authorized forceful

6. U.N. Charter art. 2(4). On its customary law nature, see Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶¶ 188–90 (June 27) [hereinafter *Nicaragua*].

7. The U.N. Secretary General has asserted that these are the only bases for the use of force. *See* U.N. Secretary General, Press Encounter on Syria, Sept. 3, 2013, http://www.un.org/sg/offthecuff/index.asp?nid=2967.

humanitarian interventions on a number of occasions, most recently during the Libyan conflict.[8]

However, every indication is that Russia and/or China would exercise their veto power as Permanent members of the Council to block an all necessary means resolution. Although it is sometimes suggested that the General Assembly may act when the Security Council is deadlocked and therefore unable to respond to a serious threat to, or breach of, international peace and security,[9] the existence of such a mechanism is legally questionable. More to the point, in the case at hand the United States would be unlikely to muster the necessary votes in the General Assembly.

B. Self-Defense

In the absence of Security Council authorization, the sole remaining textual basis for using force set forth in the Charter is self-defense pursuant to Article 51: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security." This treaty right reflects customary law.[10] States subjected to an armed attack may respond individually or seek the assistance of other States in collective self-defense. In the latter case, a State may provide assistance only once the victim State has requested it.[11]

Syria has not attacked the United States or any other State, nor is there any evidence that it intends to do so in the near future. On the contrary, such an action would be irrational given its internal turmoil. Thus, there is no basis for immediate or anticipatory self or collective defense against a paradigmatic armed attack. It is true that that the situation in Syria is destabilizing the region, particularly with respect to refugee flows into Turkey and other neighboring countries. However, contagious instability does not rise to the level of an armed attack such that the affected States may employ force in self-defense (or seek the help of other States in collective de-

8. S.C. Res. 1973 (Mar. 17, 2011). *See also*, S.C. Res. 794 (Dec. 3, 1992); S.C. Res. 814 (Mar. 26, 1993).

9. See discussion in Christina Binder, *Uniting for Peace Resolution (1950)*, MAX PLANCK ENCYCLOPEDIA OF INTERNATIONAL LAW (2006), http://opil.ouplaw.com/home/EPIL.

10. Nicaragua, *supra* note 6, ¶ 176.

11. *Id.*, ¶ 199.

fense) to stabilize the situation. And, in any event, those States have not made an official request for collective defense assistance.

The only colorable self-defense argument is that the United States may use force to preclude the possibility of chemical weapons falling into the hands of transnational terrorist groups that might use them against either the United States or its allies. Anticipatory self-defense is limited to situations in which an armed attack is "imminent." The imminency criterion had traditionally been understood as requiring temporal proximity between the impending armed attack and the forceful defensive action taken to prevent it. This is no longer the case. In light of the risk inherent in attacks involving weapons of mass destruction launched without warning,[12] an interpretation of self-defense that has gained favor allows a State to use force anticipatorily when facing an attacker who has the capability and intent to mount an armed attack once failure to act would deprive that State of an ability to defend itself.[13] In other words, the potential victim State may take forceful action if the "window of opportunity" to mount an effective defense is about to close.[14]

Applied to the Syrian situation, this threshold has not been crossed. There is no evidence that Syria intends to transfer chemical weapons to transnational terrorist groups targeting the United States or other countries. Nor has the Assad regime lost control of the country to the point where it is probable that the weapons will fall into the hands of terrorist groups. Should the latter situation occur, military operations in Syria would be permissible against the weapons and the terrorist groups in anticipatory self-defense, but not against regime targets.

---

12. This risk was first highlighted in THE WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITED STATES 15 (Nov. 2002), *available at* http://georgewbush-whitehouse.archives.gov/nsc/nss/2002/.

13. See discussion in Michael N. Schmitt, *Responding to Transnational Terrorism under the Jus ad Bellum: A Normative Framework, in* INTERNATIONAL LAW AND ARMED CONFLICT: EXPLORING THE FAULTLINES 157 (Michael N. Schmitt & Jelena Pejic eds., 2007).

14. The last window of opportunity approach was first set forth in Michael N. Schmitt, *Preemptive Strategies in International Law,* 24 MICHIGAN JOURNAL OF INTERNATIONAL LAW 524, 534–36 (2002–2003). The U.S. government has since adopted the standard. *See, e.g.*, Department of Justice White Paper, Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who is a Senior Operational Leader of Al-Qa'ida or an Associated Force, Draft, 7 (Nov. 8, 2011), http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf; Eric Holder, Attorney General, Remarks at Northwestern University School of Law, (Mar. 5, 2012), http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-1203051.html.

C. Violation of the Ban on Chemical Weapon.

The Administration has repeatedly suggested that it may act to ensure accountability for Syria's unlawful use of chemical weapons. For instance, Secretary of State Kerry has argued, "all peoples and all nations who believe in the cause of our common humanity must stand up to assure that there is accountability for the use of chemical weapons so that it never happens again."[15] The question is whether Syria's chemical attacks have normative significance—is the use of chemical weapons prohibited during non-international armed conflicts, and, if so, does this justify the use force by the United States?

Treaties promulgated as early as 1899 and 1925 banned the use of chemical weapons for parties thereto.[16] However, these earlier treaties did not extend to non-international armed conflicts. The 1993 Convention on Chemical Weapons prohibits chemical weapons use "under any circumstances,"[17] but Syria is not party to that instrument. During negotiations over the Statute of the International Criminal Court (ICC), the issue of whether to address chemical weapons use proved extremely contentious.[18] The final Statute, adopted in Rome in 1998, lists their use as a war crime during international armed conflict alone.[19]

Despite these facts, any doubt as to the existence of a norm prohibiting the use of chemical weapons in non-international armed conflict would be misplaced. The adoption of an amendment at the 2010 Kampala Review Conference filled the void in the ICC Statute by including (for States ratify-

15. John Kerry, Sec'y of State, Remarks on Syria (Aug. 26, 2013) http://www.state.gov/secretary/remarks/2013/08/213503.htm.

16. Hague Declaration (IV, 2) Concerning the Prohibition of the Use of Projectiles Diffusing Asphyxiating Gases, July 29, 1899, 26 Martens Nouveau Recueil (ser. 2) 998, 187 Consol. T.S. 453; Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, June 17, 1925, 94 L.N.T.S. 65

17. Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction, art I.1, Jan. 13, 1993, 1974 U.N.T.S. 45.

18. Neither the United States nor Syria is Party to the Statute. However, the Statute is generally considered a reliable restatement of those acts that constitute war crimes under customary international law; hence, its reference in the instant context.

19. Rome Statute of the International Criminal Court art. 8(2)(b)(xiii), July 17, 1998, 2187 U.N.T.S. 90. On the Rome Statute and chemical weapons, see Dapo Akande, *Can the ICC Prosecute for Use of Chemical Weapons in Syria?* EJIL: TALK! (Aug. 23, 2013), http://www.ejiltalk.org/can-the-icc-prosecute-for-use-of-chemical-weapons-in-syria/.

ing it) the "[employment of] asphyxiating, poisonous or other gases, and all analogous liquids, materials or devices" in the category of "serious violations of the laws and customs applicable in armed conflicts not of an international character."[20] Additionally, the International Criminal Tribunal for the former Yugoslavia has held that use of chemical weapons is unlawful during a non-international armed conflict.[21] Most importantly, the prohibition on the use of chemical weapons has undeniably crystallized into a norm of customary international law applicable in all armed conflicts. The ICRC reached this conclusion in the *Customary International Humanitarian Law* study; its characterization has not been seriously questioned.[22] And, of course, even in the absence of an express prohibition on the employment of chemical weapons, their use against the civilian population would, as with the use of any other weapon, amount to a war crime.[23] "[W]hen committed as part of a widespread or systematic attack directed against any civilian population," it would also constitute a crime against humanity.[24] The Assad regime's use of chemical weapons is indisputably a conspicuous and egregious breach of international law.

International law, however, generally provides no mechanism by which individual States may "punish" other States for violating international norms, including the prohibition on the use of chemical weapons. To some extent, that is a good thing because it limits the opportunity for subterfuge when claiming a right to use force and precludes destabilizing international vigilantism. Instead, States may only respond to an unlawful act with unfriendly but lawful measures (retorsion),[25] countermeasures not involving the use of force when they are the victim of the violation,[26] and self-

20. Amendment to Rome Statute, Art. 8(2)(e)(xiv), *available at* http://www.icc-cpi.int/iccdocs/asp_docs/Resolutions/RC-Res.5-ENG.pdf.

21. *See Tadić*, Decision on Defence Motion, *supra* note 3, ¶¶ 120–22, 124.

22. I INTERNATIONAL COMMITTEE OF THE RED CROSS, CUSTOMARY INTERNATIONAL HUMANITARIAN LAW, r.74 and accompanying commentary (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005) [hereinafter Customary IHL]. *See also* MICHAEL N. SCHMITT, CHARLES H.B. GARRAWAY & YORAM DINSTEIN, THE MANUAL ON THE LAW OF NON-INTERNATIONAL ARMED CONFLICT WITH COMMENTARY ¶ 2.2.2.c (2006); *Tadić*, Decision on Defence Motion, *supra* note 3, ¶¶ 120–22, 124.

23. Rome Statute, *supra* note 19, arts. 8(2)(c)(i) & 8(2)(e).

24. *Id.*, art. 7(1).

25. See discussion in Thomas Giegerich, *Retorsion*, MAX PLANCK ENCYCLOPEDIA OF INTERNATIONAL LAW (2001), http://opil.ouplaw.com/home/EPIL.

26. International Law Commission, Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83 annex, arts. 22, 49–54, U.N. Doc. A/RES/56/83 (Dec. 12, 2001).

defense when the violation of international law qualifies as an armed attack. Beyond these circumstances, only the Security Council wields the power to punish States for misconduct. By the terms of Article 39 of the Charter, the Council may do so whenever necessary to "maintain or restore international peace and security." In the Syrian case, robust remedies for the unlawful use of chemical weapons are therefore limited to Security Council action and to prosecution of those individuals who committed, or are otherwise responsible for, the war crimes and crimes against humanity.[27] A U.S. attack on Syria designed to hold that State accountable for its breach of international law would itself constitute an armed attack to which Syria (and other States engaging in collective self-defense at Syria's request) could respond forcefully.

D. Assistance to the Syrian Rebels

It is well accepted that during a non-international armed conflict, external States may lawfully provide military assistance to the government, although not to rebel forces.[28] But might strikes against the Assad regime be justified on the basis that the rebel forces have become the government of Syria? This is precisely the situation that prevailed once the international community recognized Karzai's government as the lawful Afghan government following the ouster of the Taliban.[29]

In November 2012, the National Coalition for Syrian Revolutionary and Opposition Forces (Syrian Opposition Council, SOC) was established. A number of States soon recognized the entity as the "legitimate representative" of the Syrian people.[30] The same month, a State Department spokesperson also labeled the SOC as the "legitimate representative of the Syrian people," a characterization repeated in December at the Friends of

27. In that Syria is not Party to the Rome Statute, prosecution before that court would require referral by the Security Council. Rome Statute, *supra* note 19, ¶ 13(b). However, the offenses are subject to universal jurisdiction, thereby affording all States the right under international law to prosecute the offenders.

28. Nicaragua, *supra* note 6, ¶ 246.

29. S.C. Res. 1419 (June 26, 2002).

30. Agreement on the Formation of the National Coalition of Syrian Revolutionary and Opposition Forces, Nov. 11, 2012. On recognition as the legitimate representative, see, e.g., E.U. Council Conclusions on Syria, 16392/12, ¶ 2, Nov. 19, 2012, http://register.consilium.europa.eu/pdf/en/12/st16/st16392.en12.pdf.

the Syrian People meeting.[31] However, in its 2012 *Digest of U.S. Practice in International Law*, the State Department explained that despite these pronouncements "the United States does not recognize the SOC as the government of Syria."[32] Having taken this stance, the Administration has closed the door to the possibility of styling military operations against Assad's forces as lawful assistance to the new government of Syria. On the contrary, and as recognized by the American Law Institute's *Restatement (3d) of Foreign Relations*, U.S. military support to a "rebellious regime . . . may violate Article 2(4) of the United Nations Charter as a use or threat of force against the political independence of the other state."[33]

E. Humanitarian Intervention

In the attendant circumstances, the sole viable legal basis for attacking Syria is humanitarian intervention.[34] The death toll since the conflict began two years ago now exceeds 100,000. Although the threshold at which the doctrine of humanitarian intervention applies is imprecise, it would seem apparent that once deaths begin to be measured in the hundreds of thousands, the line has been crossed. In this respect, the use of chemical weapons is a bit of a red herring since the number of deaths attributable to them represents a fraction of the total. Therefore, at least in the humanitarian intervention context, Syria's possession of, and demonstrated willingness to use, chemical weapons bears primarily on the issue of the likely extent of future deaths.

A legal right of humanitarian intervention is not widely accepted. Instead, States generally tend to cite a "Responsibility to Protect" (R2P).[35] By

31. Press Briefing, U.S. Department of State Deputy Spokesperson David Toner (Nov. 13, 2012), http://www.state.gov/r/pa/prs/dpb/2012/11/200477.htm#SYRIA; Office of the Legal Adviser, Dept. of State, DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW 281 (CarrieLyn D. Guymon ed., 2012), http://www.state.gov/documents/organization/211955.pdf.

32. *Id.*

33. Restatement of the Law Third: The Foreign Relations Law of the United States § 203 (1987).

34. On the subject, see Dapo Akande, *The Legality of Military Action in Syria: Humanitarian Intervention and the Responsibility to Protect,* EJIL: TALK! (Aug. 28, 2013), http://www.ejiltalk.org/humanitarian-intervention-responsibility-to-protect-and-the-legality-of-military-action-in-syria/.

35. Report of the International Commission on Intervention and State Sovereignty, THE RESPONSIBILITY TO PROTECT (Dec. 2001), http://responsibilitytoprotect.org/ICISS

R2P, States are said to bear the responsibility to protect their own nationals from harm. When they fail to do so, other States have a commensurate responsibility to take necessary measures to protect those individuals. It must be emphasized that R2P is a political mechanism and moral imperative, not a legal obligation or right. In other words, the concept provides no independent legal basis for using force to intervene in another State; to the extent the responsibility involves the use of force, that force may only be authorized through the Security Council.[36] R2P is an approach that the United States supports.[37]

By contrast, humanitarian intervention is a legal concept, albeit one that does not appear in any treaty. If the doctrine exists at all, it does so only as a matter of customary international law. States have been reticent to openly embrace the doctrine for fear that other States will misuse it in order to interfere in the affairs of their neighbors.

Despite such concerns, it can be fairly argued that the right has crystallized into customary law over the past decades. Key way points along the path of this development include international condemnation for failure to intervene in Rwanda,[38] apparent acceptance of ECOWAS interventions in Africa without Security Council authorization,[39] the NATO intervention in the Federal Republic of Yugoslavia over Kosovo, and criticism over the failure of the international community to intervene in a meaningful way in Darfur.[40] Such an argument is, of course, tenuous in light of apparent op-

---

%20Report.pdf. *See also* Gareth Evans & Mohamed Sahnoun, *The Responsibility to Protect*, FOREIGN AFFAIRS, Nov.–Dec. 2002, at 99.

36. Report of the Secretary General, Responsibility to Protect: Timely and Decisive Response, ¶¶ 138–39, UN Doc. A/66/874–S/2012/578 (July 25, 2012).

37. As set forth in the Outcome Document of the 2005 U.N. World Summit, U.N. Doc. A/RES/60/1, at ¶¶ 138–40; DIGEST OF UNITED STATES PRACTICE, *supra* note 31, at 570. *See also* United States Mission to the United Nations, Remarks by the United States at an Informal Discussion on "Responsibility while Protecting", Feb. 21, 2012, http://usun.state.gov/briefing/statements/184487.htm.

38. *See, e.g.,* Report of the Independent Inquiry into the Actions of the United Nations during the 1994 Genocide in Rwanda, Dec. 15, 1999, annexed to Letter Dated 15 December 1999 from the Secretary-General Addressed to the President of the Security Council, U.N. Doc. S/1999/1257 (Dec. 16, 1999).

39. U.N. Doc. S/22133 (Jan. 22, 1991); S.C. Res. 866 (Sept. 22, 1993); U.N. Doc. S/6481 (Feb. 26, 1998); S.C. Res. 1260 (Aug. 20, 1999).

40. The U.N. Security Council approved deployment of a peace force (United Nations Mission in Darfur—UNAMID) in 2007, but only following the signing of the Darfur Peace Agreement. S.C. Res. 1769 (July 31, 2007).

position to the doctrine by key States such as Russia and China; but it is not unreasonable.[41]

To date, the United States has not expressly acknowledged a right of humanitarian intervention. Indeed, in the case of Syria, the Administration appears to be talking around the issue. This approach stands in distinction to that adopted by our closest ally. The United Kingdom's government under Prime Minister David Cameron has officially embraced the doctrine of humanitarian intervention as providing a legal ground for operations against Syria.[42] Its position can only be based on a legal conclusion that sufficient State practice and *opinio juris* has now accumulated for a customary norm permitting humanitarian intervention to have fully matured.[43]

The U.K. has not only accepted the legal doctrine, but has articulated three conditions precedent for taking action on that basis:

> (i) there is convincing evidence, generally accepted by the international community as a whole, of extreme humanitarian distress on a large scale, requiring immediate and urgent relief;
>
> (ii) it must be objectively clear that there is no practicable alternative to the use of force if lives are to be saved; and
>
> (iii) the proposed use of force must be necessary and proportionate to the aim of relief of humanitarian need and must be strictly limited in time and scope to this aim (i.e. the minimum necessary to achieve that end and for no other purpose).[44]

It would be difficult to legally justify any humanitarian intervention not meeting these criteria. Arguably, a fourth criterion also applies. There must be some prospect of success, that is, the intervention must be likely to significantly alleviate the suffering to a degree not possible through non-

---

41. Only the United Kingdom and Belgium asserted the right of humanitarian intervention in the *Legality of the Use of Force* cases before the International Court of Justice over the Kosovo intervention. Documents on the cases are available at http://www.icj-cij.org/docket/index.php?p1=3&p2=3.

42. UK Prime Minister, Chemical Weapon Use by Syrian Regime: UK Government Legal Position, Aug. 29, 2013, https://www.gov.uk/government/publications/chemical-weapon-use-by-syrian-regime-uk-government-legal-position/chemical-weapon-use-by-syrian-regime-uk-government-legal-position-html-version.

43. North Sea Continental Shelf (FRG/Den.; FRG/Neth.), 1969 I.C.J. 3, ¶ 77 (Feb. 20).

44. UK Government Legal Position, *supr*a note 42.

forceful measures. This is a particularly relevant point in the Syrian context because President Obama has indicated that there will be no "boots on the ground" and Congress is discussing time limitations on the operations. If the conditions and restrictions ultimately imposed are so stringent that the success of the operation is drawn into question, the operation cannot qualify as a lawful humanitarian intervention.

Fulfillment of these criteria in the Syria case is a question of fact about which reasonable people may differ. However, the conclusion by Prime Minister Cameron's government that they have been met is judicious. The United States could adopt a similar legal rationale for its pending strikes against Syria.

III. CONCLUDING THOUGHTS

Absent a significant change in circumstances, there is only one possible legal basis upon which to justify military operations against Syria—humanitarian intervention.[45] Yet, the very existence of such a right in international law is highly controversial. Moreover, the United States has never explicitly accepted the doctrine *de jure*, despite invoking it *de facto* as an exceptional measure during the 1999 Kosovo intervention.

This places the United States on the horns of a dilemma. On the one hand, any avowed right of humanitarian intervention will represent key *opinio juris* that will measurably strengthen arguments that a third legal ground for using force exists in customary law. The United States should be concerned that other States might then take advantage of the doctrine for purposes that run contrary to its national interests. On the other hand, as a nation committed to the rule of law, the United States should only engage in operations consistent with international law. When legal ambiguity exists, as it does in this case, the Administration must transparently set forth its interpretation of the law justifying the use of force against other States.

In this regard, and although the U.K. Parliament rejected participation in strikes against Syria, the British government must be commended for

45. For an excellent summary of the issues discussed in this article, see Kenneth Anderson, *Legality of Intervention in Syria in Response to Chemical Weapon Attacks* 17 ASIL INSIGHTS (Aug. 30, 2013), http://www.asil.org/insights130830.cfm. On the related subject of the legality of providing arms to the Syrian rebels, see *Legitimacy Versus Legality Redux: Arming the Syrian Rebels,* 7 JOURNAL OF NATIONAL SECURITY LAW AND POLICY __ (forthcoming 2013).

taking a principled stance that its operations have to be consistent with international law, and then setting forth a reasoned interpretation of the law upon which those operations could have been based. The United States would be well served to follow suit before ordering its armed forces into action.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Arctic Climate Change and U.S. Accession to the United Nations Convention on the Law of the Sea

Raul (Pete) Pedrozo

89 INT'L L. STUD. 757 (2013)

Volume 89 2013

Arctic Climate Change and U.S. Accession to the United Nations Convention on the Law of the Sea

Raul (Pete) Pedrozo *

I. INTRODUCTION

New data released by the National Aeronautics and Space Administration (NASA)[1] and the National Oceanic and Atmospheric Administration (NOAA)[2] in 2012 and 2013 reveals that the Arctic is melting much faster than originally predicted. In September 2012, the Arctic Ocean ice pack shrank to its lowest extent on record—49 percent below the average over the past 35 years.[3] This accelerated decrease in sea ice led the Administra-

* Associate Professor, International Law Department, US Naval War College.

1. Rani Gran and Maria-José Viñas, *NASA Finds Thickest Parts of Arctic Ice Cap Melting Faster*, NASA GODDARD SPACE FLIGHT CENTER, Feb. 29, 2012, www.nasa.gov/ topics/earth/features/thick-melt.html ("A new NASA study revealed that the oldest and thickest Arctic sea ice is disappearing at a faster rate than the younger and thinner ice at the edges of the Arctic Ocean's floating ice cap."); *A change of pace*, NATIONAL SNOW AND ICE DATA CENTER, July 17, 2013, http://nsidc.org/arcticseaicenews /2013/07/a-change-of-pace/ ("During the first two weeks of July, ice extent declined at a rate . . . 61% faster than the average rate of decline over the period 1981 to 2010.").

2. Jeffries, M. O., J. A. Richter-Menge and J. E. Overland, Eds., *December 2012: Arctic Report Card 2012*, 36–42, http://www.arctic.noaa.gov/reportcard ("Sea ice extent in September 2012 reached the lowest observed in the satellite record (1979–present).")

3. Joel Clement, John Bengtson and Brendan Kelly (Lead Authors), *Managing for the Future in a Rapidly Changing Arctic*, A Report to the President from the Interagency Working

tion to re-think the need for a new national strategy to address the significant management, safety and security challenges posed by a rapidly changing Arctic environment.[4] After several months of deliberation, the White House released a new *National Strategy for the Arctic Region* on May 10, 2013 that seeks to "guide, prioritize, and synchronize efforts to protect U.S. national and homeland security interests, promote responsible stewardship, and foster international cooperation."[5] Eleven days later, the U.S. Coast Guard rolled out its new Arctic Strategy, recognizing that there will be an "increasing demand for the Coast Guard to ensure the safety, security and stewardship of the nation's arctic waters" as Arctic ice recedes and maritime activity increases.[6] The new National Strategy will also likely cause the U.S. Navy to look at its Arctic Roadmap published in 2009.[7]

The National Strategy is built on three lines of effort:

- Advance U.S. security interests;
- Pursue responsible Arctic region stewardship; and
- Strengthen international cooperation.[8]

Group on Coordination of Domestic Energy Development and Permitting in Alaska (Mar. 2013).

4. The Interagency Working Group report to the President recommended that the U.S. Government:

- Adopt an Integrated Arctic Management approach that integrates and balances environmental, economic and cultural needs and objectives when making stewardship and development decisions affecting the U.S. Arctic;
- Ensure ongoing high-level White House leadership on Arctic issues, including the development of a new National Strategy for the Arctic Region through the Presidential Policy Directive process;
- Strengthen key partnerships with the State of Alaska and Alaska Native tribal governments and organizations;
- Promote better stakeholder engagement on planning and management issues; and
- Coordinate and streamline federal action by identifying overlapping missions and reducing duplication of effort.

Id., at 3.

5. *National Strategy for the Arctic Region*, May 10, 2013, at 5, *available at* http://www.whitehouse.gov/sites/default/files/docs/nat_arctic_strategy.pdf.

6. United States Coast Guard Arctic Strategy, *The United States Coast Guard's Vision for Operating in the Arctic Region: Ensure Safe, Secure and Environmentally Responsible Maritime Activity in the Arctic*, May 21, 2013.

7. Memorandum from J.W. Greenert, Admiral, U.S. Navy, Navy Artic Roadmap (Nov. 10, 2009), Annex U.S. Navy Arctic Roadmap (Oct. 2009).

One of the key supporting objectives identified in the strategy to advance U.S. security interests is the need to preserve Arctic region freedom of the seas recognized under international law.[9] To that end, the new strategy suggests that U.S. efforts to strengthen international cooperation and partnerships can best be achieved by acceding to the 1982 *United Nations Convention on the Law of the Sea* (UNCLOS).[10]

The remaining sections of this article will analyze whether the observed acceleration of climate change in the Arctic region provides the United States with new incentives that tip the balance in favor of finally acceding to the Convention.

II. A CONSTITUTION FOR THE WORLD'S OCEANS

UNCLOS provides a comprehensive legal framework regarding uses of the oceans. Negotiated over a nine year period (1973–1982) by more than 150 delegations, UNCLOS carefully balances the interests of States to control activities off their coasts with those of all States to use the oceans without

---

8. The new strategy will be informed by the following guiding principles:

- Safeguard peace and stability;
- Make decisions using the best available information;
- Pursue innovative arrangements; and
- Consult and coordinate with Alaska Natives.

National Strategy for the Arctic Region, May 10, 2013, at 2–3.

9. The *National Strategy* states,

> The United States has a national interest in preserving all of the rights, freedoms, and uses of the sea and airspace recognized under international law. . . . Existing international law provides a comprehensive set of rules governing the rights, freedoms, and uses of the world's oceans and airspace, including the Arctic. The law recognizes these rights, freedoms, and uses for commercial and military vessels and aircraft. . . . We will also encourage other nations to adhere to internationally accepted principles.

Id., at 6.

10. The *National Strategy* states,

> Accession to the Convention would protect U.S. rights, freedoms, and uses of the sea and airspace throughout the Arctic region, and strengthen our arguments for freedom of navigation and overflight through the Northwest Passage and the Northern Sea Route. . . . While the United States is not currently a party to the Convention, we will continue to support and observe principles of established customary international law reflected in the Convention.

Id., at 6.

undue interference. Although the United States played a key role in developing the terms of the Convention consistent with U.S. national interests, President Reagan elected not to sign the treaty when it opened for signature, citing concerns with Part XI of the Convention on deep sea bed mining.[11] Despite America's refusal to sign UNCLOS, the President recognized that the Convention "contains provisions with respect to traditional uses of the oceans which generally confirm existing maritime law and practice and

---

11. President Ronald Reagan's Statement on United States Participation in the Third United Nations Conference on the Law of the Sea, Jan. 29, 1982:

> [L]ast March, I announced that my administration would undertake a thorough review of the current draft and the degree to which it met United States interests . . . Our review has concluded that while most provisions of the draft convention are acceptable and consistent with United States interests, some major elements of the deep seabed mining regime are not acceptable. . . . In the deep seabed mining area, we will seek changes necessary to correct those unacceptable elements and to achieve the goal of a treaty that:
>
> - will not deter development of any deep seabed mineral resources to meet national and world demand;
> - will assure national access to these resources by current and future qualified entities to enhance U.S. security of supply, to avoid monopolization of the resources by the operating arm of the International Authority, and to promote the economic development of the resources;
> - will provide a decision-making role in the deep seabed regime that fairly reflects and effectively protects the political and economic interests and financial contributions of participating states;
> - will not allow for amendments to come into force without approval of the participating states, including in our case the advice and consent of the Senate;
> - will not set other undesirable precedents for international organizations; and
> - will be likely to receive the advice and consent of the Senate. In this regard, the convention should not contain provisions for the mandatory transfer of private technology and participation by and funding for national liberation movements.
>
> The United States remains committed to the multilateral treaty process for reaching agreement on Law of the Sea. If working together at the Conference we can find ways to fulfill these key objectives, my administration will support ratification.

See also President Ronald Reagan's Statement on United States Oceans Policy [*hereinafter* Ocean Policy Statement], Mar. 10, 1983:

> Last July, I announced that the United States will not sign the United Nations Law of the Sea Convention that was opened for signature on December 10. We have taken this step because several major problems in the Convention's deep seabed mining provisions are contrary to the interests and principles of industrialized nations and would not help attain the aspirations of developing countries.

fairly balance the interests of all states."[12] Accordingly, the President announced that the United States was:

> prepared to accept and act in accordance with the balance of interests relating to traditional uses of the oceans—such as navigation and overflight. In this respect, the United States will recognize the rights of other states in the waters off their coasts, as reflected in the Convention, so long as the rights and freedoms of the United States and others under international law are recognized by such coastal states.[13]

Widespread recognition that the Convention's deep seabed mining regime was fundamentally flawed and required basic change in order to make it generally acceptable to the industrialized nations prompted the U.N. Secretary-General to convene a series of informal meetings in New York in 1990 to begin negotiation of a new agreement that would correct the objectionable provisions of Part XI. These efforts resulted in the adoption of the *Agreement Relating to the Implementation of Part XI of the United Nations Convention on the Law of the Sea, with Annex*.[14] The Implementing Agreement (IA) contains a number of legally binding changes that meet the six objections to Part XI raised by President Reagan in 1982. As a result, the United States and all other major industrialized nations have signed the IA.[15]

On October 7, 1994, President Clinton submitted UNCLOS and the IA to the Senate for advice and consent to accession and ratification, respectively. Despite widespread bi-partisan support, the concurrence of all the Federal agencies and departments with ocean interests, and support from the U.S. maritime industries (oil and gas, shipping, telecommunications, marine science, fishing) and environmental groups, the Convention and its Implementing Agreement have languished in the Senate for the past 20 years.

---

12. Ocean Policy Statement, Mar. 10, 1983.

13. *Id.*

14. Agreement Relating to the Implementation of Part XI of the United Nations Convention on the Law of the Sea, with Annex, Oct. 7, 1994, S. Treaty Doc. No. 103-39, 103d Cong., 2d Sess. (1994) [herenafter Annex to AI]. A/RES/48/263, July 28, 1994.

15. Letter from George P. Shultz (Secretary of State under President Reagan) to Senator Richard Lugar, June 28, 2007, http://www.jag.navy.mil/organization/code_10_law_of_the_sea.htm ("The treaty has been changed in such a way with respect to the deep seabed that it is now acceptable, in my judgment. Under these circumstances, and given the many desirable aspects of the treaty on other grounds, I believe it is time to proceed with ratification."); S. Treaty Doc. No. 103-39, at 59–60 (1994) *reprinted in* http://www.gpo.gov/fdsys/pkg/CHRG-112shrg77375/pdf/CHRG-112shrg77375.pdf.

The United States is the only major maritime power and major industrialized nation that has not joined the Convention. UNCLOS entered into force on November 16, 1994, and as of August 2013 has 166 parties. The IA entered into force on July 28, 1996, and currently has 145 parties. Although the United States is not a party to UNCLOS, it continues to view the Convention's navigational provisions as reflective of customary international law and therefore binding on all nations.[16]

Clearly, the original objections to the deep seabed mining provisions of the Convention have been rectified and are no longer grounds for objection. Thus, while the U.S. military, commercial interests and certain nongovernmental organizations have recognized and advocated for the United States to accede to the Convention for many years, the Senate has failed to act. The impacts of climate change in the Arctic region, however, should provide the necessary impetus for the U.S. Senate to revisit UNCLOS and provide its advice and consent to support U.S. accession to this important treaty.

III. BENEFITS OF JOINING UNCLOS

Since 1994, all succeeding Administrations—Democrat and Republican alike—have strongly supported U.S. accession to the Convention. UNCLOS has likewise garnered significant attention on Capitol Hill, with 13 full committee hearings devoted exclusively to UNCLOS being convened by five different Congressional committees in the last 20 years. Nonetheless, despite widespread support by all major stakeholders since the mid-1990s, proponents of the Convention have not succeeded in convincing a handful of ideologues—who continue to fallaciously view UNCLOS as an assault on U.S. sovereignty—that accession is in the best interests of the United States. The reasons for this failure are varied. First, while many of the arguments advanced by UNCLOS supporters over the years remain valid today, others have not stood the test of time or have lost much of their luster in the intervening years. Second, some UNCLOS proponents have eroded support for the Convention by articulating factually incorrect or overinflated statements in an effort to sensationalize the need to join the Convention, in the same way UNCLOS opponents argue against U.S. ratification by conjuring up the evils of the New International Economic Or-

16. This position does not allow the United States to benefit from many of the other provisions of the Convention.

der and the original flaws of Part XI. In short, having operated outside the Convention for 30 years, senators opposing accession remain unconvinced that it is still critical for the United States to accede to the Convention. Climate change in the Arctic region provides the current Administration with an opportunity to re-engage these skeptical senators with new reasons that support Senate advice and consent to accession.

A. Extended Continental Shelf Resources

As a result of melting sea ice, access to sizeable and lucrative offshore hydrocarbon and other mineral reserves in the Arctic Ocean will occur sooner than projected. Many of these resources are located beyond 200 nautical miles (nm) off the coast.

According to a 2008 assessment by the U.S. Geological Survey (USGS), "the total mean undiscovered conventional oil and gas resources in the Arctic are estimated to be approximately 90 billion barrels of oil, 1,669 trillion cubic feet of natural gas, and 44 billion barrels of natural gas liquids."[17] The overwhelming majority of these resources—84 percent—is expected to occur in offshore areas. Over 70 percent "of the mean undiscovered oil resources is estimated to occur in five provinces: Arctic Alaska, Amerasia Basin, East Greenland Rift Basins, East Barents Basins, and West Greenland-East Canada."[18] Similarly, over 70 percent "of the undiscovered natural gas is estimated to occur in three provinces: the West Siberian Basin, the East Barents Basins, and Arctic Alaska."[19] Arctic Alaska, the Amerasia Basin, and the North Chukchi-Wrangel Foreland Basin provinces, portions of which could be claimed by the United States, account for over 40 million barrels of oil, 284 billion cubic feet of natural gas, 6.5 million barrels of natural gas liquids and 94 million barrels of oil and oil-equivalent natural

17. *USGS Arctic Oil and Gas Report, Estimates of Undiscovered Oil and Gas North of the Arctic Circle*, U.S. Geological Survey Fact Sheet (July 2008).

18. *Id.*

19. *Id.*

gas.[20] The value of these resources is estimated to be in the trillions of dollars.[21]

All states may claim a 200 nm continental shelf. In addition, States Parties to UNCLOS may file claims with the Commission on the Limits of the Continental Shelf (CLCS) for exclusive sovereign rights and jurisdiction over the seabed resources of an Extended Continental Shelf (ECS) extending hundreds of miles offshore.[22] If the United States becomes a party to UNCLOS, it has strong ECS claims over the resources of the Beaufort shelf and the Chukchi shelf.[23]

Offshore oil and gas exploitation could generate thousands of U.S. jobs and billions of dollars in new government revenues, as well as extend the life of the Trans-Alaska Pipeline System (TAPS). A 2010 study conducted by Northern Economics and the University of Alaska Institute for Social and Economic Research found that developing oil and gas resources off Alaska would create an average of 54,700 new jobs per year, result in a total of $145 billion in new payroll nationwide, and generate a total of $193 billion in new government revenue.[24]

Between 1977 and 2010, TAPS supplied U.S. refineries with over 17 billion barrels of oil. However, due to the fall in production of oil in Prudhoe Bay over the past 20 years, the amount of oil flowing through the pipeline has fallen from 2.1 million to 600,000 barrels per day. According to Peter Slaiby (Vice President of Shell Alaska), "[i[f the throughput in the pipeline continues to decline and no new supplies are developed, TAPS will eventually be shut down, cutting access to one of the largest sources of domestically produced oil in the country" and increasing U.S. dependence

---

20. *Id. See also* USGS assessments in 2012 confirming these findings, *Assessment of Undiscovered Petroleum Resources of the Arctic Alaska Petroleum Province*, U.S. Geological Survey Scientific Investigations Report 2012–5147; *Assessment of Undiscovered Petroleum Resources of the Amerasia Basin Petroleum Province*, U.S. Geological Survey Scientific Investigations Report 2012–5146).

21. The price of oil and natural gas on Aug. 14, 2013 was US$106.55/bbl and US$3.36/MMBtu, respectively.

22. United Nations Convention on the Law of the Sea ("UNCLOS"), Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS], art. 76.

23. S. Treaty Doc. No. 103–39, *supra* note 15, at 56.

24. S. Hrg. 112-234, *Defending U.S. Economic Interests in the Changing Arctic: Is There a Strategy?*: Hearing before the Subcommittee on Oceans, Atmosphere, Fisheries and Coast Guard of the Committee on Commerce, Science and Transportation, United States Senate, 112th Congress, 1st Session, (July 27, 2011) (statement of Peter E. Slaiby, Vice President, Shell Alaska).

on foreign oil imports.[25] Offshore oil deposits in U.S. Arctic waters would breathe new life into TAPS.

Granted, as UNCLOS critics are quick to point out, access to the ECS under UNCLOS is contingent upon payment of royalties to the International Seabed Authority (ISBA) for oil and gas development beyond 200 nautical miles (nm).[26] However, the royalty framework is relatively insignificant compared to the fee-sharing arrangements for overseas oil and gas development and the enormous economic benefits anticipated from offshore resource development. Revenue sharing does not begin until the 6th year of production of a particular well or site, starts at 1% of the value of production and increases 1% per year. By the 12th year and remaining years thereafter, the royalty is 7% of the value of production, paid either in kind or in dollars.[27] During the 1970s, these revenue sharing provisions were negotiated in consultation with the U.S. oil and gas industry.

Payments are to be distributed by the ISBA to States Parties of UNCLOS in accordance with Article 82(4) on the basis of equitable criteria that take into account economic development factors. Of note, this distribution is distinct from the distribution of revenues generated from deep seabed mining operations under Part XI of the Convention. As a State Party to UNCLOS, the United States would have a permanent seat in the ISBA to ensure both kinds of distributions are made in ways acceptable to the United States—Section 3(15) of the Annex to the IA guarantees the United States a seat on the ISBA Council in perpetuity.[28] Any ISBA decision regarding revenue sharing must be approved by the Council.[29] Additionally, if distributions are made to a country that is already receiving U.S. foreign aid, the United States could offset aid to that country by the amount of distributions paid by the ISBA, in essence eliminating any increase financial burden to the American taxpayers.

Critics suggest accession to UNCLOS is not required in order for the United States to claim an ECS, since the 1958 Continental Shelf Convention and the 1945 Truman Proclamation already support a unilateral U.S.

---

25. *Id.*

26. UNCLOS, *supra* note 22, art. 82.

27. *Id.*.

28. Annex to AI, *supra* note 14, Section 3(15) (providing that the State with the largest economy in terms of gross domestic product as of November 16, 1994, is guaranteed a seat on the Council).

29. Annex to IA, *supra* note 14, Section 3(5); UNCLOS, *supra* note 22,, arts. 161(8)(d) & 162(2)(o).

claim. Although that may be true, the metric for determining the outer extent of the ECS is more generous in UNCLOS than in the 1958 Convention or the Truman Proclamation, both of which rely on an "exploitability criterion" to identify the outer limit of the ECS.[30] More importantly, the U.S. oil and gas industry believes that unilaterally claiming an ECS outside UNCLOS may be challenged by other nations in courts throughout the world, and has therefore repeatedly argued that legal certainty/security of tenure to explore and exploit the resources of the ECS can be obtained only through UNCLOS.[31] The bottom line is that U.S. industry will not invest in offshore oil and gas production in the ECS unless the United States is a party to UNCLOS.[32]

---

30. Convention on the Continental Shelf, art. 1, Apr. 29, 1958, 499 U.N.T.S. 311:

> For the purpose of these articles, the term 'continental shelf' is used as referring (a) to the seabed and subsoil of the submarine areas adjacent to the coast but outside the area of the territorial sea, to a depth of 200 metres or, beyond that limit, to where the depth of the superjacent waters admits of the exploitation of the natural resources of the said areas; (b) to the seabed and subsoil of similar submarine areas adjacent to the coasts of islands.

See also Proclamation 2667—Policy of the United States With Respect to the Natural Resources of the Subsoil and Sea Bed of the Continental Shelf, Sept. 28, 1945.

31. Convention on the Law of the Sea, S. Exec. Rpt. No. 110–9, Committee on Foreign Relations (Dec. 19, 2007) at 9:

> In an era when the United States faces growing energy vulnerability, failing to accede to the Convention will constrain the opportunities of U.S. energy companies to explore beyond 200 nm. Mr. Paul Kelly, testifying on behalf of the oil and gas industry, asserted that under the Convention, the United States would have the opportunity to receive international recognition of its economic sovereignty over more than 291,000 square miles of extended continental shelf. Much of this is in the Arctic, which holds approximately one quarter of the world's undiscovered oil and natural gas, according to the U.S. Geological Survey World Petroleum Assessment in 2000.

32. U.S. Dep't of State Press Release, Statement of Secretary of State Hillary Rodham Clinton, The Law of the Sea Convention (Treaty Doc. 103-39): The U.S. National Security and Strategic Imperatives for Ratification, The U.S. National Security and Strategic Imperatives for Ratification (May 23, 2012), *at* http://www.state.gov/secretary/rm/2012/05/190685.htm:

> U.S. oil and gas companies are now ready, willing, and able to explore this area. But they have made it clear to us that they need the maximum level of international legal certainty before they will or could make the substantial investments, and, we believe, create many jobs in doing so needed to extract these far-offshore resources. If we were a party to the convention, we would gain international recognition of our sovereign rights, including by using the convention's procedures, and therefore be able to give our oil and gas companies this legal certainty. Staying outside the convention, we simply cannot.

The sea-bed and ocean floor beyond the limits of national jurisdiction—that is, beyond the 200 nm continental shelf or beyond the ECS established pursuant to UNCLOS—to include all resource exploration and exploitation activities, are regulated by the ISBA, in accordance with Part XI of the Convention and the Part XI IA. If the United States continues to delay establishing the outer limit of its ECS in the Arctic, other nations may undercut U.S. claims and receive ISBA license to extract resources in areas that otherwise could be under exclusive U.S. jurisdiction.

In May 2013, five Asian nations—including China—were granted observer status in the Arctic Council, and China has stated it does not intend to be a "wallflower" in the forum.[33] Beijing has expressed an interest in developing new shipping routes through the Arctic that will connect China with its largest export market—the European Union. To that end, in August 2013, a Chinese merchant vessel loaded with heavy equipment and steel set sail from Dalian en route to Rotterdam via the Arctic's Northern Sea Route (NSR).[34] China has also expressed an interest in developing Arctic resources. In March 2010, Rear Admiral Yin Zhou of the People's Liberation Army Navy stated at the Eleventh Chinese People's Political Consultative Conference that "under . . . UNCLOS, the Arctic does not belong to any particular nation and is rather the property of all the world's people" and that "China must play an indispensable role in Arctic exploration as it has one-fifth of the world's population."[35] Officials from the State Oceanic Administration have similarly indicated that China is a "near Arctic state" and that the Arctic is an "inherited wealth for all humankind."[36] As a party to UNCLOS, the United States could claim an ECS in the Arctic and forestall any encroachment of U.S. ocean resources by China or any other nation.

---

33. Linda Jakobson, *Preparing for an ice-free Arctic*, CHINA DIALOGUE, Apr. 21, 2010 (Although China recognizes that the Arctic is primarily a regional issue, the Assistant Minister of Foreign Affairs indicated in a speech at an Arctic forum in 2009 on Svalbard that "concerns over climate change and international shipping gave [the Arctic] inter-regional dimensions.").

34. Bill Savadove, *China reveals its Arctic ambitions in new shipping route*, JAPAN TIMES, Aug. 18, 2013.

35. Jakobson, *supra* note 33.

36. Bhavna Singh, *China And The Arctic: The Next 'Strategic' Frontline?*, EURASIA REVIEW, Oct. 19, 2012.

B. Freedom of Navigation

U.S. freedom of navigation interests in the Arctic would be bolstered by joining UNCLOS. Both Russia and Canada have maritime claims in the Arctic that are inconsistent with the rules contained in the Convention.

Russia[37] and Canada[38] draw excessive straight baselines in the Arctic and restrict the right of transit passage in various international straits in the Arctic, including the Northeast Passage, the Northwest Passage and various straits located within Russia's Northern Sea Route (NSR)—the Demitri, Laptev and Sannikov Straits. Russia's straight baselines closing the NSR straits and Canada's straight baselines around its Arctic Islands do not meet the legal criteria contained in Article 7 of the Convention.[39] According to UNCLOS Article 5, the correct baseline for these areas is the low-water line. UNCLOS Article 38 also provides that the right of transit passage through international straits cannot be suspended or impeded by the bordering States. Use of straight baselines by Russia and Canada to close these international straits is therefore inconsistent with the Convention. Furthermore, under UNCLOS Article 8(2), all nations enjoy at least the right of innocent passage in areas within newly drawn straight baselines.

The United States has diplomatically protested and operationally challenged these excessive straight baseline claims under the U.S. Freedom of Navigation Program, citing the provisions of UNCLOS and customary in-

37. List of Geographical Coordinates of the Points Determining the Baselines Position for Measuring the Breadth of the Territorial Waters, Economic Zone and Continental Shelf of the USSR, Adopted by Decrees of the USSR Council of Ministers on Feb. 7, 1984; List of Geographical Coordinates of the Points Determining the Baselines Position for Measuring the Breadth of the Territorial Waters, Economic Zone and Continental Shelf of the USSR, Adopted by Decrees of the USSR Council of Ministers on Jan. 15, 1985; Federal Act on the internal maritime waters, territorial sea and contiguous zone of the Russian Federation**,** Adopted by the State Duma on July 16, 1998, Approved by the Federation Council on July 17, 1998.

38. Territorial Sea Geographical Coordinates (Area 7) Order, P.C., SOR/1985–872 (Can.).

39. UNCLOS, *supra* note 22, article 7 states,

> In localities where the coastline is deeply indented and cut into, or if there is a fringe of islands along the coast in its immediate vicinity, the method of straight baselines joining the appropriate points may be employed in drawing the baseline from which the breadth of the territorial sea is measured.

ternational law.[40] However, the U.S. legal position would be on better footing if the United States was a party to the Convention.

Russia and Canada have also enacted domestic laws and regulations to regulate maritime traffic in their Arctic waters, citing UNCLOS Article 234 as their legal basis.[41] Although Article 234 does allow coastal States to adopt and enforce measures to prevent, reduce and control vessel-source pollution in ice-covered areas, such measures must have "due regard to navigation." Both the Russian and Canadian laws and regulations in question, however, exceed what is permissible under international law, including the Safety of Life at Sea Convention (SOLAS)[42] and UNCLOS. They also exceed current International Maritime Organization (IMO) construction, design, equipment and manning (CDEM) standards set out in the IMO Polar Code.[43]

Russia's NSR regulations[44] and Canada's Northern Canada Vessel Traffic Service Zone Regulations (NORDREGS)[45] were unilaterally adopted without IMO approval. However, mandatory ship routing,[46] mandatory

---

40. U.S. Dep't of Defense, *Maritime Claims Reference Manual*, DOD 2005.1-m (June 23, 2005), *available at* http://www.jag.navy.mil/organization/code_10_mcrm.htm.

41. UNCLOS, *supra* note 22, art. 234 (Ice-covered areas) provides:

> Coastal States have the right to adopt and enforce non-discriminatory laws and regulations for the prevention, reduction and control of marine pollution from vessels in ice-covered areas within the limits of the exclusive economic zone, where particularly severe climatic conditions and the presence of ice covering such areas for most of the year create obstructions or exceptional hazards to navigation, and pollution of the marine environment could cause major harm to or irreversible disturbance of the ecological balance. Such laws and regulations shall have due regard to navigation and the protection and preservation of the marine environment based on the best available scientific evidence.

42. International Convention for the Safety of Life at Sea, Annex, Ch. V, Reg. 33(1), Nov. 1, 1974, T.I.A.S. No. 9700 [hereinafter SOLAS].

43. Guidelines for Ships Operating in Polar Waters, IMO Doc.A26/Res. 1024 Annex (Dec. 2, 2009), *available at* http://www.imo.org/blast/blastDataHelper.asp?data_id=29985&filename=A1024(26).pdf.

44. Regulations for Navigation on the Seaways of the Northern Sea Route, Approved by the USSR Minister of Merchant Marine, Sept. 14, 1990; Requirements for Design, Equipment and Supply of Vessels Navigating the Northern Sea Route; 1996 Regulations for Icebreaker and Pilot Guiding of Vessels Through the Northern Sea Route.

45. Northern Canada Vessel Traffic Services Zone Regulations, Canada Gazette, Vol. 144, No. 9, Feb. 27, 2010.

46. SOLAS, *supra* note 42, Regulation V/10 provides, in part,

> 1. . . . Ships' routing systems . . . may be made mandatory . . . when adopted and implemented in accordance with the guidelines and criteria developed by the . . . [IMO]. 2. . . . Contracting

ship reporting[47] and mandatory vessel traffic services (VTS)[48] that apply beyond the 12-nm territorial sea of a coastal State must be submitted to and approved by the IMO under SOLAS Chapter V. SOLAS Regulations V/10(9) and V/11(8) further provide that all routing and reporting "systems and actions taken to enforce compliance with those systems shall be consistent with international law, including . . . [UNCLOS]."

Coastal State maritime traffic regulations adopted by the IMO must also be applied consistent with the right of transit passage guaranteed to all ships and aircraft by Part III of UNCLOS.[49] To the extent that the Russian and Canadian regulations require compulsory pilotage and prior permission to transit international straits, they violate UNCLOS Articles 38 and 42, which prohibit coastal States from adopting domestic measures that impede or "have the practical effect of denying, hampering or impairing the right of transit passage."[50]

Application of domestic environmental laws and regulations adopted pursuant to Article 234 is also subordinate to UNCLOS Article 236, which exempts all sovereign immune vessels from the environmental provisions of the Convention.[51] NORDREGS exempts warships from compliance;

> Governments shall refer proposals for the adoption of ships' routeing systems to the…[IMO]. . . . 4. Ships' routeing systems should be submitted to the . . . [IMO] for adoption.

47. SOLAS, *supra* note 42, Regulation V/11 (providing, in part, "[a] ship reporting system, when adopted and implemented in accordance with the guidelines and criteria developed by the . . . [IMO] . . ., shall be used by all ships. . . . Contracting Governments shall refer proposals for the adoption of ship reporting systems to the . . . [IMO]."

48. SOLAS, *supra* note 42, Regulation V/12 stipulates, in part, "[the use of VTS may only be made mandatory in sea areas within the territorial seas of a coastal State."

49. SOLAS, *supra* note 42, Regulations V/10(10), V/11(9) and V/12(5) (providing that "[n]othing in this regulation nor its associated guidelines and criteria shall prejudice the rights and duties of Governments under international law or the legal regimes of straits used for international navigation and archipelagic sea lanes.").

50. Of note, on August 23, 2013, a Greenpeace icebreaker—the *Arctic Sunrise*—set sail for the Arctic to challenge Russia's prior permission regime for the NSR after being denied a permit to transit the Russian waterway on three previous occasions. Bob Weber, *Greenpeace to defy Russians, enter Arctic seas without permit*, THE CANADIAN PRESS, Aug. 26, 2013.

51. UNCLOS, *supra* note 22, art. 236 (Sovereign immunity):

> The provisions of this Convention regarding the protection and preservation of the marine environment do not apply to any warship, naval auxiliary, other vessels or aircraft owned or operated by a State and used, for the time being, only on government non-commercial service. However, each State shall ensure, by the adoption of appropriate measures not impairing operations or operational capabilities of such vessels or aircraft owned or operated by it, that such

however, other government sovereign immune vessels are not exempt. The NSR regulations do not exempt sovereign immune vessels from the duty to comply. To the extent that the Russian and Canadian laws and regulations apply to sovereign immune vessels, they are inconsistent with international law, including UNCLOS Article 236 and SOLAS, Regulation V/1.[52]

As a party to UNCLOS, U.S. opposition to these unilateral laws and regulations would be strengthened to include the possibility of compulsory dispute settlement under Part XV of the Convention. Application of these domestic measures in the EEZ and in international straits clearly interferes with U.S. high seas freedoms of navigation and overflight and other lawful uses of the seas. Such actions also exceed IMO-approved rules and standards for the protection of the marine environment in the EEZ. Moreover, neither government has provided sufficient data to demonstrate that their domestic laws and regulations are based on the best available scientific evidence, as required by UNCLOS Article 234. The Convention's compulsory dispute settlement procedures can be invoked by a State Party for a number of reasons, including interference with high seas freedoms of navigation and overflight and other lawful uses of the sea in the EEZ (Article 297(1)(a)) and contravention of international rules and standards for the protection and preservation of the marine environment in the EEZ (Article 297(1)(c)).

C. American Leadership

The United States has historically been the world leader in protecting the common interest in navigational freedom and the rule of the law in the oceans. However, America has temporarily lost that leadership by its con-

---

vessels or aircraft act in a manner consistent, so far as is reasonable and practicable, with this Convention.

52. Consistent with UNCLOS, *supra* note 22, art. 234, SOLAS, *supra* note 42, Regulation V/1 states, in part:

> Unless expressly provided otherwise, this chapter shall apply to all ships on all voyages, except: .1 warships, naval auxiliaries and other ships owned or operated by a Contracting Government and used only on government non-commercial service . . . . However, warships, naval auxiliaries or other ships owned or operated by a Contracting Government and used only on government non-commercial service are encouraged to act in a manner consistent, so far as reasonable and practicable, with this chapter.

tinued non-adherence to UNCLOS. U.S. accession to the Convention will restore that role and advance U.S. leadership in Arctic Ocean issues.

Joining UNCLOS will put the United States on an even footing with the other Arctic nations, as America assumes the chairmanship of the Arctic Council from Canada in 2015. All of the Council's member States (except the United States) and its 12 observer States are parties to the Convention. Moreover, in 2008, the five Arctic coastal States (Canada, Denmark, Russia, Norway and the United States) declared at Ilulissat that the law of the sea, as reflected in UNCLOS, is the legal framework that governs the Arctic Ocean, and there is no need for a new legal regime to govern the Arctic Ocean.[53] Therefore, U.S. participation in the Arctic Council recognizes UNCLOS as the governing framework in the Arctic.

The Arctic Council provides a forum for promoting cooperation, coordination and interaction among the Arctic States on common Arctic issues, in particular issues of sustainable development and environmental protection. The Council adopted an Arctic Search and Rescue (SAR) agreement in 2011[54] and an Arctic oil response agreement in 2013,[55] both of which take into account the relevant provisions of UNCLOS. The member States of the Arctic Council are also leading the way for the development of a mandatory Polar Code at the IMO that will give context to UNCLOS Article 234, while giving due regard to navigation.

Similarly, the Council will have an increasing role in developing management regimes for Arctic fisheries beyond areas of national jurisdiction. Although there are currently no commercial fisheries in the Arctic, salmon and other fish are expected to move north as global warming alters sea ice

---

53. The Ilulissat Declaration, Arctic Ocean Conference, Ilulissat, Greenland, May 27-28, 2008:

> [T]he law of the sea provides for important rights and obligations concerning the delineation of the outer limits of the continental shelf, the protection of the marine environment, including ice-covered areas, freedom of navigation, marine scientific research, and other uses of the sea. We remain committed to this legal framework and to the orderly settlement of any possible overlapping claims. This framework provides a solid foundation for responsible management by the five coastal States and other users of this Ocean through national implementation and application of relevant provisions. We therefore see no need to develop a new comprehensive international legal regime to govern the Arctic Ocean.

54. Arctic Council's Agreement on Cooperation on Aeronautical and Maritime Search and Rescue in the Arctic, May 12, 2011, *available at* http://www.library.arcticportal.org/1474/1/Arctic_SAR_Agreement_EN_FINAL_for_signature_21-Apr-2011.pdf.

55. Arctic Council's Agreement on Cooperation on Marine Oil Pollution Preparedness and Response in the Arctic, May 15, 2013.

conditions.[56] This northern migration will result in a concomitant increase in the number of fishing vessels operating further north of their traditional fishing grounds. Increased fishing activities in the region could lead to increased foreign incursions into the U.S. EEZ, as well as overfishing in areas beyond the EEZs of the other Arctic States. As a result, in 2009, the United States imposed a moratorium on commercial fishing in the Arctic Management Area—U.S. Federal waters north of the Bering Strait in the Chukchi and Beaufort Seas—until more information is available to support sustainable fisheries management.[57]

Nevertheless, the United States cannot "go it alone" in the Arctic—it will need the cooperation of the other member States of the Arctic Council to ensure that U.S. conservation efforts initiated with the Arctic Fisheries Management Plan are not put in jeopardy. The Council's work in this regard will be informed by the provisions of UNCLOS relating to the conservation and management of straddling fish stocks and highly migratory fish stocks (Articles 63 and 64), as well as the 1995 Straddling Fish Stocks and Highly Migratory Fish Stocks Agreement, which elaborates on the fundamental principles of conservation and management established in UNCLOS Articles 116-120.

U.S. leadership in evaluating other nations ECS claims in the Arctic is also lacking. As a non-Party to UNCLOS, the United States is not only precluded from filing an ECS claim with the CLCS, it also cannot participate in the CLCS process to evaluate and make recommendations on other States' ECS claims in the Arctic and elsewhere. Russia submitted an Arctic ECS claim to the CLCS in 2001 (partially revised in February 2013).[58] In February 2002, the United States filed a notification with the United Nations regarding the Russian submission, indicating that it lacks sufficient

56. Joel Clement, John Bengtson and Brendan Kelly (Lead Authors), *Managing for the Future in a Rapidly Changing Arctic*, A Report to the President from the Interagency Working Group on Coordination of Domestic Energy Development and Permitting in Alaska (Mar. 2013).

57. Fisheries of the United States Exclusive Economic Zone off Alaska; Fisheries of the Arctic Management Area; Bering Sea Subarea, 74 FR 56734, Nov. 3, 2009.

58. Commission on the Limits of the Continental Shelf (CLCS) Outer limits of the continental shelf beyond 200 nautical miles from the baselines: Submissions to the Commission: Submission by the Russian Federation, Dec. 20, 2001, and Commission on the Limits of the Continental Shelf (CLCS) Outer limits of the continental shelf beyond 200 nautical miles from the baselines: Submissions to the Commission: Partial revised Submission by the Russian Federation, Feb. 28, 2013, http://www.un.org/depts/los/clcs_new/commission_submissions.htm.

scientific data to support Russia's ECS claim in the Arctic.[59] The U.S. notification also invoked UNCLOS, stressing "the importance of promoting stability of relations in the oceans, and of complying with the provisions of Article 76 of . . . [UNCLOS]."

However, as a non-Party to UNCLOS, the United States lacks standing to challenge other nations' excessive claims in the Arctic citing the provisions of the Convention. The same is true in other regions of the world. China, for example, continues to pursue an aggressive posture in the South China Sea and routinely criticizes the United States for not being a Party to UNCLOS—"the U.S. insists that China must base its [South China Sea] claims solely on the 1982 UNCLOS although the U.S. itself has not ratified it."[60] Similarly, when Iran signed UNCLOS in 1982, it filed a declaration indicating, *inter alia*, that "only states parties to the Law of the Sea Convention shall be entitled to benefit from the contractual rights created therein, [including] the right of Transit passage through straits used for international navigation."[61] Thus, Iran argues that the United States does not enjoy a right of transit passage through the Strait of Hormuz because that right is contractual in nature. Joining the Convention would put the United States on solid legal ground to conclusively "put to bed" these assertions.

IV. Conclusion

The United States has basic and enduring national interests in the oceans. These diverse interests—security, economic, scientific, dispute settlement, environmental, and leadership—are best protected through a comprehensive, widely accepted international agreement that governs the varying (and sometimes competing) uses of the sea. Although the United States has lived outside the Convention for 30 years, climate change in the Arctic provides the current Administration with a new and urgent incentive to reengage the Senate and urge that body to provide its advice and consent to

59. United States of America: Notification regarding the submission made by the Russian Federation to the Commission on the Limits of the Continental Shelf, CLCS.01.2001.LOS/USA, Mar. 18, 2002, http://www.un.org/depts/los/clcs_new/commission_submissions.htm ("The United States believes that the submission has major flaws as it relates to the continental shelf claim in the Arctic.").

60. Mark Valencia, *The South China Sea: What China Could Say*, NAPSNet Policy Forum, May 7, 2013.

61. Declaration by the Islamic Republic of Iran upon signing the 1982 United Nations Convention on the Law of the Sea, Dec. 10, 1982, http://www.un.org/depts/los/ convention_agreements/convention_declarations.htm.

U.S. accession to the treaty at the earliest opportunity. As a nation with both coastal and maritime interests, the United States would benefit immensely from becoming a party to UNCLOS—accession will restore U.S. oceans leadership, protect U.S. ocean interests and enhance U.S. foreign policy objectives, not only in the Arctic, but globally.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

The Syrian Crisis and the Principle of *Non-Refoulement*

Mike Sanderson

89 INT'L L. STUD. 776 (2013)

Volume 89 2013

The Syrian Crisis and the Principle of *Non-Refoulement*

Mike Sanderson[*]

I. FACTUAL BACKGROUND

On April 25, 2011, the Syrian military entered Daraa with a force of up to 5,000 men and seven T-55 tanks and began an operation to suppress the political opposition there.[1] The southern city of Daraa first became the focus of political opposition to the Assad regime in March 2011 when some 15 local school children were arrested for painting anti-government slogans on the walls of a school.[2] Protests spread quickly across the country to Jassem,[3] Da'el,[4] Sanamein,[5] Inkhil[6] and then Damascus.[7] Government security

---

* Lecturer in Law, School of Law, University of Exeter.

1. *Syrian Army Attacks Protest City of Daraa*, BBC NEWS (Apr. 25, 2011), http://www.bbc.co.uk/news/world-middle-east-13185185.

2. Joe Sterling, *Daraa: The spark that Lit the Syrian Flame*, CNN (Mar. 1, 2012), http://edition.cnn.com/2012/03/01/world/meast/syria-crisis-beginnings/index.html.

3. *Thousands March in Syria, as Fresh Wave of Protests Erupts*, THE TELEGRAPH (Mar. 21, 2011), http://www.telegraph.co.uk/news/worldnews/middleeast/syria/8395679/Thousands-march-in-Syria-as-fresh-wave-of-protests-erupts.html.

4. *Syrian Security Forces Fire on Protestors; Eight Killed*, CNN (May 28, 2011), http:// edition.cnn.com/2011/WORLD/meast/05/27/syria.unrest/index.html.

forces had already responded with the wide-spread detention and torture of protesters and, in some cases, live fire.[8] Heavy armor was first used on April 25, 2011,[9] marking the descent into civil war.[10]

The ensuing humanitarian consequences for the people of Syria have been dreadful.[11] Estimates by the United Nations High Commissioner for Human Rights (OHCHR) place the number now killed at upwards of 100,000 people.[12] Over five million have been internally displaced[13] and more than two million people have sought refuge abroad.[14] While the intensity of violence has driven some Syrians to seek refuge further afield,[15]

---

5. Khaled Yacoub Oweis, *Protests Spread Against Assad Rule in Syria* REUTERS (Mar. 25, 2011), http://www.reuters.com/article/2011/03/25/us-syria-idUSTRE72N2MC20110325.

6. Katherine Marsh, *Syria: Four Killed in Deraa as Protests Spread Across South*, THE GUARDIAN (Mar. 22, 2011), http://www.theguardian.com/world/2011/mar/22/syrian-protests-troops-kill-deraa.

7. *The Revolution Reaches Damascus*, FOREIGN POLICY (Mar. 18, 2011), http://www.foreignpolicy.com/articles/2011/03/18/the_revolution_reaches_damascus.

8. For a narrative timeline of the initial stages of the anti-Assad protest movement see HUMAN RIGHTS WATCH, "WE'VE NEVER SEEN SUCH HORROR", CRIMES AGAINST HUMANITY BY SYRIAN SECURITY FORCES 8–13 (2011), http://www.hrw.org/sites/ default/files/reports/syria0611webwcover.pdf.

9. *Syrian Army Attacks Protest City of Daraa*, *supra* note 1.

10. *Syrian Arab Republic*, *in* 2012 ANNUAL REPORT 443 (ICRC, 2012), http://www.icrc.org/eng/assets/files/annual-report/current/icrc-annual-report-syria.pdf (last visited Oct. 1, 2013) [hereinafter ICRC 2012 Annual Report] ("What had started out as localized clashes between the Syrian government and armed groups in 2011 gradually evolved into a non-international armed conflict in 2012.").

11. Regular humanitarian bulletins on the situation in Syria are prepared by the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) and may be found on their *Syria Crisis* site: http://www.unocha.org/crisis/syria (last visited Oct. 1, 2013).

12. *Syria Death Toll Now Above 100,000, Says UN Chief Ban*, BBC NEWS (July 25, 2013), http://www.bbc.co.uk/news/world-middle-east-23455760.

13. The most recent statistics on internal displacement in Syria are available at the Syria page of the Internal Displacement Monitoring Centre (IDMC), http://www.internal-displacement.org/8025708F004CE90B/(httpCountries)/9F19CC00280C471C802570A7004CE12F?OpenDocument (last visited Oct. 1, 2013).

14. Up to date statistics on "persons of concern" to the United Nations High Commissioner for Refugees (UNHCR) seeking refuge abroad are available at the Syria Regional Refugee Response Inter-agency Information Sharing Portal, http://data.unhcr.org/syrian refugees/regional.php (last visited Oct. 1, 2013).

15. Boris Cheshirkov, *Bulgaria's Asylum Centres Bursting at the Seams as Syrian Refugees Enter Europe*, UNHCR (Sept. 17, 2003), http://www.refworld.org/docid/52396d074.html. OCHA estimates that a further 28,000 people have now fled to various countries in Europe, see *Syria* 34 OCHA HUMANITARIAN BULLETIN 9 (Sept. 10–23, 2013),

the vast majority of Syrians remain in the five key countries of refuge surrounding Syria: Egypt, Iraq, Jordan, Lebanon and Turkey.[16] Each country has responded to the recent influx of civilians fleeing the violence in Syria with outstanding generosity. Lebanon, in particular, has consistently maintained an open-door policy towards those seeking refugee from the Syrian violence.[17] The resulting impact on Lebanese society has been marked.[18] As of October 3, 2013, UNHCR estimates that there are now 779,038 Syrians seeking protection in Lebanon, up from some 20,000 in May 2012.[19] This is in addition to the 425,000 Palestinian refugees registered in Lebanon prior to the war in Syria and the further 50,000 Palestinian refugees who arrived in Lebanon following their displacement from refugee camps in Syria.[20] To put this in some perspective, with the overall Lebanese population estimated at 4.2 million,[21] the number of refugees in Lebanon now amounts to almost a quarter of the total Lebanese population.[22]

In these circumstances it would be naïve to expect such generosity to persist indefinitely. Egypt, Iraq, Jordan and Turkey have begun to actively limit the number of Syrians permitted to seek refuge on their territory by imposing quotas on those allowed to cross the border from Syria each day, refusing entry to particular classes as defined in relation to gender and/or age or by closing the border altogether.[23] Those Syrians prevented from

---

http://reliefweb.int/sites/reliefweb.int/files/resources/Syria%20Humanitarian%20Bulletin%20No%2034.pdf (last visited Oct. 1, 2013).

16. A detailed statistical breakdown of the caseload in each country can be found on the Inter-agency Information Sharing Portal, *supra* note 14. As of October 3, 2013 there were 127,411 Syrian persons of concern in Egypt, 195,068 in Iraq, 536,405 in Jordan, 779,038 in Lebanon and 502,827 in Turkey.

17. *Inter-agency Regional Response for Syrian Refugees*, UNHCR, 1 (Sept. 19–25, 2013), http://www.refworld.org/docid/52452f244.html.

18. *See Lebanon: Economic and Social Impact Assessment of the Syrian Conflict*, WORLD BANK (Report No. 81098, Sept. 20, 2013), http://documents.worldbank.org/curated/en/2013/09/18292074/lebanon-economic-social-impact-assessment-syrian-conflict.

19. Inter-agency Information Sharing Portal, *supra* note 14.

20. *Id.*; Caroline Abu Sa'Da and Michaela Serafini, *Humanitarian and Medical Challenges of Assisting New Refugees in Lebanon and Iraq*, 44 FORCED MIGRATION REVIEW 70 (2013).

21. *Country Profile Lebanon*, UNDATA http://data.un.org/CountryProfile.aspx?crName=LEBANON (last visited Oct. 1, 2013).

22. It will, in fact, be a somewhat lower proportion as the most recent estimate of the Lebanese population has not yet been corrected to reflect the current influx. Nevertheless, the proportion remains extraordinarily high.

23. *Egypt: Do Not Return Asylum Seekers to Syria*, HUMAN RIGHTS WATCH (July 10, 2013), http://www.hrw.org/news/2013/07/10/egypt-do-not-return-asylum-seekers-syria:

crossing are left exposed to the worst effects of the conflict and, in particular, the depredations of the Syrian military, which now seems increasingly inclined to directly attack border areas.[24] However, States must, nonetheless, seek to comply with the legal requirements pertaining to refugees within the limits of their capacity. It is therefore, of the first importance to identify public international law resources that bind States experiencing a refugee influx.

Any discussion concerning refugees must begin with the right against forced return or *non-refoulement* found in the 1951 Refugee Geneva Convention.[25] This article therefore first examines the terms of the 1951 Refugee Convention and its application in the surrounding States of Egypt, Lebanon and Turkey (Section II). Particular attention is given to the new (2013) Turkish Law on Foreigners,[26] which transposes many of the most im-

---

> Without prior warning, on July 8, the Egyptian government changed its entry policy for Syrians arriving in Egypt by requiring them to obtain a visa and security clearance before arriving in the country. According to media reports, on the same day Egypt denied entry to 276 people arriving from Syria, including a plane with Syrian nationals on board, who were then flown back to the Syrian town of Latakia.

Jordan: Obama Should Press King on Asylum Seeker Pushbacks, HUMAN RIGHTS WATCH (Mar. 21, 2013), http://www.hrw.org/news/2013/03/21/jordan-obama-should-press-king-asylum-seeker-pushbacks ("Jordan is routinely and unlawfully rejecting Palestinian refugees, single males, and undocumented people seeking asylum at its border with Syria, said Human Rights Watch and Harvard Law School's International Human Rights Clinic (the Harvard Clinic) today."); Tom Peter, *Egypt, Jordan, Iraq Seek to Stem Syrian Refugee Flood*, CHRISTIAN SCIENCE MONITOR (July 14, 2013), http://www.csmonitor.com /World/Middle-East/2013/0714/Egypt-Jordan-Iraq-seek-to-stem-Syrian-refugee-flood:

> While the International Rescue Committee commends Syria's neighbours for maintaining an open borders policy, we are increasingly concerned about reports of Syrians having difficulty entering Turkey, Jordan and Iraq. The international community should strongly encourage hosting governments and the Syrian regime to respect the right of all refugees fleeing Syria to 'seek and enjoy asylum' and discourage policies – including the closure of borders – that prevent civilians from leaving Syria," says Ned Colt, regional communications manager for the International Rescue Committee.

Syria, *in* WORLD REPORT 2013, 609, 612 (Human Rights Watch, 2013), *available at* http: //www.hrw.org/world-report/2013/country-chapters/syria; Abu Sa'Da and Serafini, *supra* note 20, at 70.

24. *Syrian Warplane Attacks Lebanese Border Area*, AL-JAZEERA (Aug. 3, 2013), http:// www.aljazeera.com/news/middleeast/2013/08/20138313050777721.html.

25. Convention Relating to the Status of Refugees art. 33, Apr. 22, 1954, 189 U.N.T.S. 137 [hereinafter 1951 Refugee Convention].

26. Law on Foreigners and International Protection Law, 2013, No. 6458 (Turk.) [hereinafter Law on Foreigners]. An unofficial English translation of this law prepared by UNHCR is available at http://www.refworld.org/docid/5167fbb20.html (last visited Oct. 8, 2013).

portant elements of the 1951 Refugee Convention into Turkish domestic law. The section then turns its focus to the so-called "nexus requirement" found in the 1951 Convention,[27] examining the role this limitation might have in the Syrian context. The latter half of the article moves beyond the terms of the 1951 Convention to discuss parallel sources of protection, including prospects for a regional protection instrument (Section III), the principle of *non-refoulement* in general international human rights law (Section IV), customary international law (section V) and international humanitarian law (Section VI).

Only a minority of the States surrounding Syria are party to either the 1951 Convention or the 1967 Protocol to the Convention[28] or have passed domestic asylum/refugee laws implementing anything like the provisions of the Convention in respect of *non-refoulement*. Even where States are parties to one of the treaties the obligations either remain unimplemented or, where relevant domestic legislation has been passed, ineffective for the protection of refugees. Nevertheless, reference to both general international human rights and humanitarian law discloses an extensive set of legal norms which, if used effectively, will support a very comprehensive right of *non-refoulement* for individuals displaced from Syria to the surrounding States.

II. THE 1951 REFUGEE CONVENTION AND DOMESTIC LAW IN THE SURROUNDING STATES

The basic legal instruments for the protection of refugees are the 1951 Refugee Convention and the 1967 Protocol to the Convention. Read together they define the concept of a refugee for the purposes of international law and set forth the rights attendant to refugee status. A refugee is defined in Article 1(A)2 of the Convention as a person who,

> As a result of events occurring before 1 January 1951 and owing to well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his nationality and is unable, or owing to such fear, is unwilling to avail himself of the protection of that country. . . .

27. 1951 Refugee Convention, *supra* note 25, art. 1(A)(2).

28. Protocol Relating to the Status of Refugees, Oct. 4, 1967, 606 U.N.T.S. 267 [hereinafter 1967 Protocol].

The Convention limits application of the term "refugee" to those fleeing due to "events occurring before 1 January 1951" and provides an option to States parties of further limiting the definition to those fleeing due to "events occurring in Europe."[29] A similar definition, although not restricted to events occurring in Europe or before 1951, is incorporated into the Statue of the Office of the United Nations High Commission for Refugees (UNHCR Statute).[30] Rather than creating a new definition, the 1967 Protocol commits States parties to implementing Article 1(A)2 of the 1951 Refugee Convention without the chronological (events occurring prior to 1951) or geographic (events occurring in Europe) restrictions,[31] save where the geographic limitation is explicitly preserved by States parties to the Protocol.[32]

The principle of *non-refoulement*, or the prohibition on forced return, found in 1951 Refugee Convention is integral to any discussion of entry for those fleeing persecution:

> 1. No Contracting State shall expel or return ("refouler") a refugee in any manner whatsoever to the frontiers of territories where his life or freedom would be threatened on account of his race, religion, nationality, membership of a particular social group or political opinion;
>
> 2. The benefit of the present provision may not, however, be claimed by a refugee whom there are reasonable grounds for regarding as a danger to the security of the country in which he is, or who, having been convicted by a final judgment of a particularly serious crime, constitutes a danger to the community of that country. [33]

---

29. 1951 Refugee Convention, *supra* note 25, art. 1(B)(1):

> For the purposes of this Convention, the words "events occurring before 1 January 1951" in article 1, section A, shall be understood to mean either (a) "events occurring in Europe before 1 January 1951"; or (b) "events occurring in Europe or elsewhere before 1 January 1951"; and each Contracting State shall make a declaration at the time of signature, ratification or accession, specifying which of these meanings it applies for the purpose of its obligations under this Convention.

30. Statute of the Office of the United Nations High Commissioner for Refugees, G.A. Res. 428 (V), art. 6(A)(ii), U.N. GAOR, 5th Sess., Supp. No. 20, at 46 U.N. Doc. A/1775 (Dec. 14, 1950) [hereinafter UNHCR Statute], art. 6(B); for a concise explanation of the differences between the UNHCR Statute and the 1951 Refugee Convention see JAMES C. HATHAWAY, THE LAW OF REFUGEE STATUS 12 n. 56 (1991).

31. 1967 Protocol, *supra* note 28, art. 1(2).

32. *Id.*, art. 1(3).

33. 1951 Refugee Convention, *supra* note 25, art. 33.

As an injunction framed in "negative terms,"[34] the *non-refoulement* provisions of the 1951 Convention do not provide a right of entry *per se*. However, insofar as admission to the territory of the asylum State will, in practice, often be the only way to avoid returning an asylum-seeker to the "frontiers of territories where his life or freedom would be threatened,"[35] this will frequently amount to a *de facto* right of admission.[36]

However, of the five key reception States surrounding Syria, only Egypt and Turkey are States parties to either the 1951 Refugee Convention or the 1967 Protocol to the Convention[37] and only Lebanon and Turkey have passed domestic laws governing the definition and protection of asylum-seekers and refugees.[38] Although there are now 144 States parties to the 1951 Refugee Convention and 145 to the 1967 Protocol, countries in the Middle East and North Africa (MENA) region continue to have a very low rate of accession to either treaty. In large part this is due to the continuing concern among Arab States with the issue of Palestinian refugees.

In fact, Arab States supported the exclusion of Palestinian refugees from the terms of the 1951 Refugee Convention and the UNHCR Statute.[39] These States were concerned that if Palestinian refugees were included in the terms of either document they "would become submerged [with other categories of refugees] and would be relegated to a position of minor importance."[40] The 1951 Refugee Convention establishes a model of protection in displacement based on the fundamental right of *non-refoulement*. In contrast with the fear of persecution and the right of *non-refoulement* that

34. *Applicant M38/2002* v. *Minister for Immigration and Multicultural and Indigenous Affairs* [2003] FCR 131, ¶ 39 (Austl.).

35. 1951 Refugee Convention, *supra* note 25, art. 33.

36. James C. Hathaway, *Refugees and Asylum*, *in* FOUNDATIONS OF INTERNATIONAL MIGRATION LAW 177, 193 (Brian Opeskin, Richard Perruchoud & Jillyanne Redpath, eds., 2012).

37. UNHCR *States Parties to the 1951 Convention relating to the Status of Refugees and the 1967 Protocol*, as of Apr. 1, 2011, http://www.unhcr.org/protect/PROTECTION/3b73b0d63.pdf.

38. Law on Foreigners, *supra* note 26; *Loi réglementant l'entrée et le séjour des étrangers au Liban ainsi que leur sortie de ce pays* (Law Regulating the Entry and Stay of Foreigners in Lebanon and their Exit from the Country (Law of Entry and Exit) Bulletin de Législation Libanaise (Journal Officiel), 1962, No. 28-1962, art. 26 (Leb.).

39. OROUB EL-ABED, UNPROTECTED: PALESTINIANS IN EGYPT SINCE 1948 163 (2009); 1951 Refugee Convention, *supra* note 25, art. 1(d); UNHCR Statute, *supra* note 32, art. 7(c).

40. LEX TAKKENBERG, THE STATUS OF PALESTINIAN REFUGEES IN INTERNATIONAL LAW 66 (1998).

concerns many asylum-seekers, Palestinian refugees demand a right to return to Palestine in line with the terms of General Assembly Resolution 194.[41] Arab States have been hesitant to accede to the Convention as, in part, it fails to present a model of protection relevant to the needs of Palestinians.[42]

A. Egypt and Lebanon

Although Egypt is a party to both the 1951 Refugee Convention and the 1967 Protocol, it has not yet promulgated relevant domestic asylum law or developed the procedures or institutions necessary to comply with their obligations under the Convention.[43] In accordance with a memorandum of understanding signed with the UNHCR in 1954 the government has devolved virtually all aspects of refugee protection, including the provision of social welfare and status determination, to the UNHCR.[44]

The provisions of the 1962 Lebanese law are restricted quite specifically to granting political asylum only[45] and so would most likely exclude any claims made by the Syrians fleeing civil disorder and violence in their own country. However, this remains a matter of speculation as no steps have been taken to implement these provisions through either the promulgation of regulations or the development of State institutions for the determina-

---

41. G.A. Res. 194 (III), ¶ 11 U.N. Doc. A/RES/194 (III) (Dec. 11, 1948):

> Resolves that the refugees wishing to return to their homes and live at peace with their neighbours should be permitted to do so at the earliest practicable date, and that compensation should be paid for the property of those choosing not to return and for loss of or damage to property which, under principles of international law or in equity, should be made good by the Governments or authorities responsible.

See also Ben Lynfield, *As Peace Talks Pick Up, Palestinians Demand a Return to Villages Fled Long Ago,* CHRISTIAN SCIENCE MONITOR (Aug. 18, 2013), http://www.csmonitor.com/World/Middle-East/2013/0818/As-peace-talks-pick-up-Palestinians-demand-a-return-to-villages-fled-long-ago.

42. Jaber Suleiman, *Trapped Refugees: the Case of Palestinians in Lebanon*, *in* NO REFUGE: PALESTINIANS IN LEBANON 11 (Refugee Studies Centre, Working Paper Series No. 64, 2010), http://www.rsc.ox.ac.uk/publications/working-papers-folder_contents/RSCworkingpaper64.pdf.

43. *Global Report 2012: Egypt*, UNHCR, http://www.refworld.org/docid/4e52379612.html (last visited Oct. 8, 2013).

44. Michael Kagan, *"We Live in a Country of UNHCR": The UN Surrogate State and Refugee Policy in the Middle East*, (UNHCR, New Issues in Refugee Research, Research Paper No. 201, Feb. 2011), http://www.refworld.org/docid/4d8876db2.html.

45. Law Regulating the Entry and Stay of Foreigners, *supra* note 40, art. 26.

tion of refugee claims and/or the protection of asylum-seekers. As such, the Lebanese State continues to treat all asylum-seekers as, in essence, illegal immigrants and extends its protection to them on a wholly discretionary basis.[46]

B. The New Turkish Law on Foreigners

While Turkey has acceded to the 1967 Protocol it continues to limit its protection obligations to those persons fleeing persecution as a result of "events occurring in Europe."[47] This restriction, reflected in the new Turkish law, excludes those fleeing the Syrian conflict.[48] However, the new law introduces an, admittedly discretionary, provision for the temporary protection of individuals in the context of mass influx.[49] There is also provision for the subsidiary protection of individuals who do not come within

46. HUMAN RIGHTS WATCH, ROT HERE OR DIE THERE: BLEAK CHOICES FOR IRAQI REFUGEES IN LEBANON 16 (2007), http://www.hrw.org/sites/default/files/reports/lebanon1207.pdf:

> Lebanon treats people who enter illegally to seek asylum, or who enter legally but then overstay their visas for the same purpose, as illegal immigrants who are subject to imprisonment, fines, and deportation. The situation improved significantly with the September 2003 Memorandum of Understanding (MOU) between Lebanon's General Security and UNHCR. While the MOU declares that "Lebanon does not consider itself as an asylum country" and that "the only viable durable solution for refugees recognized under the mandate of UNHCR is resettlement in a third country," the MOU seeks to provide "temporary humanitarian solutions for the problems of people entering clandestinely, residing unlawfully in Lebanon and submitting asylum applications at UNHCR.

47. 1967 Protocol, *supra* note 28, art. 1(3); States Parties, *supra* note 39, at 5; JAMES C. HATHAWAY, THE RIGHTS OF REFUGEES UNDER INTERNATIONAL LAW 97 (2005); Dilek Latif, *Refugee Policy of the Turkish Republic*, 33 TURKISH YEARBOOK OF INTERNATIONAL RELATIONS 1 (2002).

48. Law on Foreigners, *supra* note 26, art. 61:

> A person who as a result of events occurring in European countries and owing to well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group or political opinion, is outside the country of his or her nationality and is unable or, owing to such fear, is unwilling to avail himself or herself of the protection of that country; or who, not having a nationality and being outside the country of his or her former habitual residence as a result of such events, is unable or, owing to such fear, is unwilling to return to it shall be recognized as a refugee following the refugee status determination procedures.

49. *Id.*, art. 91(1) ("Temporary protection *may be provided* to foreigners who, having been forced to leave their country and cannot return to the country they left, have arrived at or crossed the borders of Turkey in masses seeking emergency and temporary protection.") (emphasis added).

the terms of the domestic refugee definition. Individuals who may face "the death penalty or execution,"[50] torture or inhuman or degrading treatment or punishment"[51] or a "serious threat to his or her person by reason of indiscriminate violence"[52] upon return to his or her country of origin, are protected by the law.

Like the 1951 Refugee Convention itself, the Turkish law has a standalone *non-refoulement* provision. Unfortunately, however, it is framed in a manner so inconsistent with the other elements of the law as to be virtually inscrutable. Article 4 of the new law forbids return "to a place where he or she may be subject to torture, inhuman or degrading punishment or treatment, or where his or her life or freedom may be under threat."[53] However, while Article 4 purports to extend this guarantee to all individuals who fall "under the scope of this Law,"[54] it goes on to limit the actual effect of the *non-refoulement* provision to those individuals whose "life or freedom may be under threat on account of [their] race, religion, nationality, membership of a particular social group or political opinion."[55] This clause appears to restrict the provision's application to those defined as refugees in Article 61 of the law, thereby excluding individuals granted subsidiary protection pursuant to Article 63 or temporary protection pursuant to Article 91 from its gamut. As will be recalled, the refugee definition in Article 61 is itself limited to those fleeing "events occurring in Europe," but this restriction is not reflected in Article 4. The end result is that the Article 4 *non-refoulement* provision is in some way inconsistent with each of the new law's qualification provisions.

It is difficult to understand at this stage whether the terms of the new law reflect a considered legislative scheme or is merely the result of poor and inconsistent drafting. One possibility is that the *non-refoulement* provision (insofar as it excludes the "geographical limitation") is intended to be

50. *Id.*, art. 63(1)(a).

51. *Id.*, art. 63(1)(b); *cf* Convention for the Protection of Human Rights and Fundamental Freedoms art. 3, Nov. 4, 1950, 213 U.N.T.S. 222 [hereinafter ECHR].

52. Law on Foreigners, *supra* note 26, art. 63(1)(c); *cf* Council Directive 2011/95/EU on Standards for the Qualification of Third-Country Nationals or Stateless Persons as Beneficiaries of International Protection, for a Uniform Status for Refugees or for Persons Eligible for Subsidiary Protection, and for the Content of the Protection Granted (Recast), art. 15, 2011 O.J. (L 337); C-465/07, Elgafaji v. Staatssecretaris van Justitie, 2009 E.C.R. I-00921 [hereinafter EU Qualification Directive].

53. Law on Foreigners, *supra* note 26, art. 4.

54. *Id.*

55. *Id.*

broader in scope than the Article 61 qualification provision. However, in that case it is hard to see what advantage there is in retaining this limitation in respect of the qualification provision itself. Moreover, there seems little point in adding further grounds for subsidiary protection in Articles 63 and 91 if those in receipt of such protection do not benefit from the guarantee against *non-refoulement*.

Until this law is implemented by the Turkish State its practical effect will remain a matter of speculation. However, the process of implementation bears careful scrutiny, particularly in respect to those seeking protection due to a "serious threat to [their] person by reason of indiscriminate violence."[56] Should Article 4, as implemented, give protection from *refoulement* to those entitled to subsidiary protection within the meaning of this article (and, by extension, a *de facto* right of entry), this will mark the development of a key resource for the protection of individuals fleeing civil disorder in the Middle East.

C. The "Nexus Requirement"

Any regime for the protection of individuals fleeing the violence in Syria premised on either the 1951 Convention or the domestic law of the key receiving States suffers from two key protection gaps. First, as noted, only two out of the five States (Egypt and Turkey) are States parties to the two key international refugee protection instruments; neither of which has, as yet, begun to implement the instruments in a comprehensive manner. Second, even where the provisions of these instruments bind the receiving States, it remains unclear whether Syrians seeking protection in these States will have refugee claims consistent with the requirements of Article 1(A)2 of the 1951 Convention.[57] This latter issue warrants further discussion, particularly in light of the UNHCR's recent approach with respect to those fleeing the Syrian conflict.

In order to qualify for refugee status under the Article 1(A)2 definition, the "well-founded fear of persecution" must be "*for reasons of* race, religion, nationality, membership of a particular social group or political opinion." The persecution feared must be causally related to one of the grounds

56. *Id.*, art. 63(1)(c).

57. 1951 Refugee Convention, *supra* note 25, art. 1(A)(2). See discussion at section II.

enumerated in Article 1(A)2.[58] This is commonly referred to as the "causal nexus."[59] While some Syrians have certainly fled their country due to a well-founded fear of persecution for reasons of religion[60] or political opinion,[61] in accordance with Article 1(A)2 of the Refugee Convention, many will have fled due to their fear of generalized violence and civil disorder unrelated to a Convention ground. The question is, can this "causal nexus" be established as a result of generalized violence?

This is not to suggest, however, that there is a requirement to show a differential impact on those fleeing civil situations of conflict of large-scale civil disorder or that such a finding is limited to any particular number of individuals.[62] There is no basis in the text of the 1951 Convention to impose a higher or differential burden on claimants seeking to make out a claim to refugee status in the context of armed conflict.[63] Moreover, while the Convention ground must contribute meaningfully to the cause of the persecution feared, it need not be the sole or even the predominant cause of that persecution.[64]

---

58. James C. Hathaway, *The Michigan Guidelines on Nexus to a Convention Ground*, 23 MICHIGAN JOURNAL OF INTERNATIONAL LAW 211, 213, ¶ 1 (2002) [hereinafter Michigan Guidelines].

59. *Id.*, at 219, ¶ 17.

60. Patrick Cockburn, *Persecution of the Christians: Syrian Minority Fear the End of Fighting More than War Itself*, THE INDEPENDENT (Dec. 17, 2012), http://www.independent.co.uk/news/world/middle-east/persecution-of-the-christians-syrian-minority-fear-the-end-of-fighting-more-than-war-itself-8422977.html; Clarissa Ward, *Syria's Christians Fearing Religious Persecution*, CBS NEWS (Feb. 21, 2013), http://www.cbsnews.com/video/watch/?id=50141509n.

61. *Syria: Political Detainees Tortured, Killed*, HUMAN RIGHTS WATCH (Oct. 3, 2013), http://www.hrw.org/news/2013/10/03/syria-political-detainees-tortured-killed.

62. UNHCR, *Eligibility Guidelines for Assessing the International Protection Needs of Iraqi Asylum-Seekers* 133 (2007), http://www.refworld.org/docid/46deb05557.html ("Whole communities may risk or suffer persecution for Convention reasons. The fact that all members of the community are equally affected does not in any way undermine the legitimacy of any particular individual claim."); Michigan Guidelines, *supra* note 60, at 218, ¶ 16; Michael Kagan and William P. Johnson, *Persecution in the Fog of War: The House of Lords' Decision in Adan*, 23(2) MICHIGAN JOURNAL OF INTERNATIONAL LAW 247 (2002).

63. Vanessa Holzer, *The 1951 Refugee Convention and the Protection of People Fleeing Armed Conflict and Other Situations of Violence*, UNHCR Division of International Protection Legal and Protection Policy Research Series 16, PPLA/2012/05 (Sept. 2012) http://www.unhcr.org/504748069.pdf.

64. Michigan Guidelines, *supra* note 60, at 218, ¶ 13; Michelle Foster, *Causation in Context: Interpreting the Nexus Clause in the Refugee Convention*, 23(2) MICHIGAN JOURNAL OF INTERNATIONAL LAW 265 (2002).

The significance of a particular ground is to be judged subjectively by reference to the perspective of the persecutor (rather than the refugee).[65] It is the views of the persecutor that are relevant for establishing the causal nexus and determining the reasons that motivate particular conduct (i.e., acts of persecution).[66] This follows from the wording of Article 1(A)2, which requires the persecution to be "for reasons of" a Convention ground. It is irrelevant for the purposes of establishing the nexus whether the particular ground is true or has merely been imputed to the refugee (rightly or wrongly) or, indeed, whether the ground of persecution is known to the refugee at all.[67] If a persecutor acts on a belief related to an enumerated Convention ground then this suffices to establish the causal nexus regardless of whether that belief is mistaken or, indeed, implausible.[68]

Finally, it must be emphasized that the standards relevant to the determination of the causal nexus are general and no particular or special requirements apply where the refugees originate from a country in which there is widespread violence or civil disorder. While asylum-seekers from a country in this position are not automatically refugees, they are entitled to recognition on the same terms as any asylum-seeker where they meet the requirements of Article 1(A)2.[69] Indeed, in the view of UNHCR,

> most Syrians seeking international protection are likely to fulfil the requirements of the refugee definition contained in Article 1A(2) of the 1951 Convention relating to the Status of Refugees, since they will have a well-founded fear of persecution linked to one of the Convention

65. Andreas Zimmermann and Claudia Mahler, *Art. 1 A para. 2*, *in* THE 1951 CONVENTION RELATING TO THE STATUS OF REFUGEES AND ITS 1967 PROTOCOL: A COMMENTARY 281, ¶ 426 (Andreas Zimmerman, ed., 2011); Attorney General v. Ward [1993] 2 S.C.R. 689, 747 (Can.).

66. Zimmerman and Mahler, *supra* note 67, ¶ 427.

67. GUY GOODWIN-GILL AND JANE MCADAM, THE REFUGEE IN INTERNATIONAL LAW 87 (2007); U.N. High Comm'r for Refugees, *Guidelines on International Protection No.1: Gender-Related Persecution within the context of Article 1A(2) of the 1951 Convention and/or its 1967 Protocol relating to the Status of Refugees*, ¶¶ 22–23, U.N. Doc. HCR/GIP/02/01 (May 7, 2002); U.N. High Comm'r for Refugees, *Guidelines on International Protection No. 6: Religion-Based Refugee Claims under Article 1A(2) of the 1951 Convention and/or the 1967 Protocol relating to the Status of Refugees*, ¶ 31, U.N. Doc. HCR/GIP/04/06 (Apr. 28. 2004); U.N. High Comm'r for Refugees, *Guidelines on International Protection No. 8: Child Asylum Claims under Articles 1(A)2 and 1(F) of the 1951 Convention and/or 1967 Protocol relating to the Status of Refugees*, ¶¶ 46–47, U.N. Doc. HCR/GIP/09/08 (Sept. 22, 2009).

68. Zimmerman and Mahler, *supra* note 67, ¶ 428.

69. Michigan Guidelines, *supra* note 60, at 219, ¶ 17.

> grounds. For many civilians who have fled Syria, the nexus to a 1951 Convention ground will lie in the direct or indirect, real or perceived association with one of the parties to the conflict.[70]

If one takes the subjectivity of the Convention grounds seriously it will admit of the sweeping and even erratic imputation of particular grounds to broad sections of a community. The question is not whether such imputations are accurate or even plausible but whether they serve to motivate the conduct of the persecutors. As UNHCR explains in reference to Syria,

> parties to the conflict reportedly employ broad interpretations of whom they may consider as being associated with the other party, including based on an individual's family links, religious or ethnic background or mere presence in an area considered as being "pro-" or "anti-Government." This is illustrated by the methods and tactics of warfare that have been documented in Syria and include, *inter alia*, the systematic besieging, bombarding, raiding, pillaging and destruction of residences and other civilian infrastructure in whole neighbourhoods, purportedly for reason of real or perceived support to the other conflict party.[71]

This account is both plausible and laudably sensitive to the particular conditions of the Syrian conflict. It is consistent with the subjectivity of the Convention grounds to admit of their attribution on even very general terms. Certainly this would include the grounds provided by the UNHCR, of "family links, religious or ethnic background or mere presence in an area." In any case, there is not yet a settled body of case law in respect of their refugee status. As such, any conclusions as to the correct application of the causal nexus in this context must remain somewhat speculative.

III. NO REGIONAL PROTECTION INSTRUMENT

The protection situation is aggravated by the absence of a regional refugee instrument akin to the European Union (EU) Qualification Directive[72] or the Organization of African Unity (OAU) Refugee Convention.[73] These

70. U.N. High Comm'r for Refugees, *International Protection Considerations with Regard to People Fleeing the Syrian Arab Republic, Update II,* ¶ 14 (Oct. 22, 2013), www.refworld.org/docid/5265184f4.html.

71. International Protection Considerations Syria, *supra* note 72, at 8, n.56.

72. EU Qualification Directive, *supra* note 54.

73. Organization of African Unity (OAU) Convention Governing the Specific Aspects of Refugee Problems in Africa, Sept. 10, 1969, 1001 U.N.T.S. 45.

both make specific provision for the protection of individuals fleeing large-scale violence or civil disorder, albeit in somewhat different terms.[74] There is, in fact, a draft Arab League Refugee Convention[75] which makes provision for the protection of individuals displaced ". . . because of sustained aggression against, occupation and foreign domination of such country or because of the occurrence of natural disasters or grave events resulting in major disruption of public order."[76] However, this Convention has never enjoyed significant political support in the Arab world and no State has yet ratified it.[77] As such, it remains in draft form with little prospect of change in the foreseeable future.

IV. INTERNATIONAL HUMAN RIGHTS LAW

The available protection regime can be significantly enhanced by reference to general standards of international human rights law. Of particular importance in this context are the International Covenant on Civil and Political Rights (ICCPR)[78] and the Convention against Torture (CAT).[79] All of the five key receiving States are parties to both conventions.[80] The conven-

---

74. EU Qualification Directive, *supra* note 54, art. 15(c):

> Serious harm consists of: (a) the death penalty or execution; or (b) torture or inhuman or degrading treatment or punishment of an applicant in the country of origin; or (c) serious and individual threat to a civilian's life or person by reason of indiscriminate violence in situations of international or internal armed conflict.

OAU Refugee Convention, *supra* note 75, art. 1(2):

> The term "refugee" shall also apply to every person who, owing to external aggression, occupation, foreign domination or events seriously disturbing public order in either part or the whole of his country of origin or nationality, is compelled to leave his place of habitual residence in order to seek refuge in another place outside his country of origin or nationality.

75. League of Arab States, *Arab Convention on Regulating Status of Refugees in the Arab Countries* 1994, http://www.refworld.org/docid/4dd5123f2.html (last visited Oct. 9, 2013).

76. *Id.*, art. 1.

77. Suleiman, *supra* note 44, at 16.

78. International Covenant on Civil and Political Rights, Mar. 23, 1976, 999 U.N.T.S. 171 [hereinafter ICCPR].

79. Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, June 26, 1987, 1465 U.N.T.S. 85 [hereinafter CAT].

80. A complete list of States party to the CAT and the ICCPR can be found on the website of the United Nations Treaty Collection, at http://treaties.un.org (last visited Oct. 9, 2013).

tions contain absolute and non-derogable[81] rights against torture[82] and, in the case of the ICCPR, the arbitrary deprivation of life.[83] Significantly, the CAT includes an explicit right against *non-refoulement* in Article 3(1):

> No State Party shall expel, return ("*refouler*") or extradite a person to another State where there are substantial grounds for believing that he would be in danger of being subjected to torture.

Moreover, the Human Rights Committee has found a guarantee against *refoulement* to be implicit in the meaning of Article 7 of the ICCPR.[84]

The guarantees contained in both the ICCPR and the CAT go considerably beyond torture *per se* to address a broader variety and degree of ill-treatment. This is important to note in the context of forced displacement, as both conventions extend the assurances against *refoulement* to situations where ill-treatment is feared. The (non-derogable) Article 1 guarantee

---

81. CAT, *supra* note 81, art. 2(2); ICCPR, *supra* note 80, art. 4(2). *See also* Committee against Torture General Comment 2: Implementation of Article 2 by States Parties U.N. Doc. CAT/C/GC/2/CRP.1/Rev.4, ¶ 5 (2007):

> Article 2, paragraph 2, provides that the prohibition against torture is absolute and non-derogable. It emphasizes that *no exceptional circumstances whatsoever* may be invoked by a State Party to justify acts of torture in any territory under its jurisdiction. The Convention identifies as among such circumstances, a state of war or threat thereof, internal political instability or any other public emergency. This includes any threat of terrorist acts or violent crime as well as armed conflict, international or non-international.

82. CAT, *supra* note 81, arts. 1, 2; ICCPR, *supra* note 80, art. 7.

83. ICCPR, *supra* note 80, art. 6.

84. U.N. Human Rights Committee General Comment 20: Article 7 (44th Sess.), U.N. Doc. HRI/GEN/1/Rev.1 at 30, ¶ 9 (1992):

> In the view of the Committee, States parties must not expose individuals to the danger of torture or cruel, inhuman or degrading treatment or punishment upon return to another country by way of their extradition, expulsion or refoulement. States parties should indicate in their reports what measures they have adopted to that end.

U.N. Human Rights Committee General Comment 31: Nature of the General Legal Obligation Imposed on States Parties to the Covenant (80th Sess.) U.N. Doc. CCPR/C/21/Rev.1/Add.13, ¶ 12 (1994):

> . . . the article 2 obligation requiring that States Parties respect and ensure the Covenant rights for all persons in their territory and all persons under their control entails an obligation not to extradite, deport, expel or otherwise remove a person from their territory, where there are substantial grounds for believing that there is a real risk of irreparable harm, such as that contemplated by articles 6 and 7 of the Covenant, either in the country to which removal is to be effected or in any country to which the person may subsequently be removed.

against torture[85] in the CAT is supplemented by the broader (albeit, derogable) Article 16 guarantees against "cruel, inhuman or degrading treatment,"[86] while Article 7 of the ICCPR incorporates both elements into a non-derogable guarantee against ill-treatment.[87] The Committee against Torture[88] and the Committee on Human Rights[89] have sought to minimize any potential distinctions among the various categories of ill-treatment. The Committee against Torture, in particular, has emphasized that the obligation to prevent all forms of ill-treatment addressed by the CAT are interdependent, indivisible and interrelated.[90] As explained in its General Comment 2,

> . . . the definitional threshold between ill-treatment and torture is often not clear. Experience demonstrates that the conditions that give rise to ill-treatment frequently facilitate torture and therefore the measures required to prevent torture must be applied to prevent ill-treatment. Accordingly, the Committee has considered the prohibition of ill-treatment to be likewise non-derogable under the Convention and its prevention to be an effective and non-derogable measure.[91]

---

85. CAT, *supra* note 81, art. 1:

> For the purposes of this Convention, the term "torture" means any act by which severe pain or suffering, whether physical or mental, is intentionally inflicted on a person for such purposes as obtaining from him or a third person information or a confession, punishing him for an act he or a third person has committed or is suspected of having committed, or intimidating or coercing him or a third person, or for any reason based on discrimination of any kind, when such pain or suffering is inflicted by or at the instigation of or with the consent or acquiescence of a public official.

86. CAT, *supra* note 81, art. 16:

> Each State Party shall undertake to prevent in any territory under its jurisdiction other acts of cruel, inhuman or degrading treatment or punishment which do not amount to torture as defined in article 1, when such acts are committed by or at the instigation of or with the consent or acquiescence of a public official or other person acting in an official capacity.

87. ICCPR, *supra* note 80, art. 7 ("No one shall be subjected to torture or to cruel, inhuman or degrading treatment or punishment. In particular, no one shall be subjected without his free consent to medical or scientific experimentation.").

88. Committee against Torture General Comment 2, *supra* note 83, ¶ 3.

89. U.N. Human Rights Committee General Comment 20, *supra* note 86, ¶ 4:

> The Covenant does not contain any definition of the concepts covered by article 7, nor does the Committee consider it necessary to draw up a list of prohibited acts or to establish sharp distinctions between the different kinds of punishment or treatment; the distinctions depend on the nature, purpose and severity of the treatment applied.

90. Committee against Torture General Comment 2, *supra* note 83, ¶ 3.

91. *Id.*, ¶ 3.

The guarantee against the arbitrary deprivation of life found in Article 6 of the ICCPR is equally broad in scope. While Article 6 itself refers to both the death penalty[92] and the crime of genocide,[93] the Committee on Human Rights has evinced particular concern with the threat to life posed by armed conflict. As the Committee explains in its General Comment 6,

> The right to life enunciated in article 6 of the Covenant has been dealt with in all State reports. It is the supreme right from which no derogation is permitted even in time of public emergency which threatens the life of the nation (art. 4). However, the Committee has noted that quite often the information given concerning article 6 was limited to only one or other aspect of this right. It is a right which should not be interpreted narrowly.
>
> The Committee observes that war and other acts of mass violence continue to be a scourge of humanity and take the lives of thousands of innocent human beings every year . . . The Committee considers that States have the supreme duty to prevent wars, acts of genocide and other acts of mass violence causing arbitrary loss of life. Every effort they make to avert the danger of war, especially thermonuclear war, and to strengthen international peace and security would constitute the most important condition and guarantee for the safeguarding of the right to life.[94]

The relevance of these provisions as interpreted to the current situation in Syria is plain given the widespread allegations of human rights abuses.[95] Both conventions contain guarantees against *refoulement* to situations where ill-treatment is feared. However, and as distinct from the 1951 Refugee Convention, there is no requirement to establish a causal nexus between the ill-treatment feared and the particular grounds or reasons for that ill-treatment. The guarantees against ill-treatment in both the CAT and the ICCPR, including the rights of *non-refoulement*, are absolute and unrelated to

---

92. ICCPR, *supra* note 80, art. 6(2).

93. *Id.*, art. 6(3).

94. U.N. Human Rights Committee General Comment 6: Article 6 (16th Sess.) U.N. Doc. HRI\GEN\1\Rev.1, ¶¶ 1–2 (1982).

95. HUMAN RIGHTS WATCH, TORTURE ARCHIPELAGO: ARBITRARY ARRESTS, TORTURE, AND ENFORCED DISAPPEARANCES IN SYRIA'S UNDERGROUND PRISONS SINCE MARCH 2011 (2012): http://www.hrw.org/sites/default/files/reports/syria0712webwcover.pdf; Stephanie Nebehay, *Syrian Forces Responsible for Banias Massacres: UN Report*, REUTERS (Sept. 11, 2013), http://www.reuters.com/article/2013/09/11/us-syria-crisis-warcrimes-idUSBRE98A0D5 20130911.

any particular grounds or causes. The breadth of these guarantees makes them especially valuable in situations of armed conflict where assessing the reasons or motivations relevant to the causal nexus can be particularly difficult.

V. A PARALLEL CUSTOMARY INTERNATIONAL NORM

Running alongside these conventional norms is a broad customary international norm of *non-refoulement*.[96] This will continue to bind States even after they accede to a treaty that to some degree reflects the customary international norm.[97] In this case the norms run in parallel to one another and, assuming they are not inconsistent,[98] may be applied in the alternative.[99] Inevitably the two categories of norms will be closely related, with conventional norms serving as the clearest possible evidence of the *opinio juris* of States.[100] As calculated by Bethlehem and Lauterpacht, "170 of the 189 members of the UN, or around 90 per cent of the membership, are party to one or more conventions which include *non-refoulement* as an essential

96. As early as 1977 the UN Executive Committee (ExComm) on the International Protection of Refugees noted that ". . . the fundamental humanitarian principle of non-refoulement has found expression in various international instruments adopted at the universal and regional levels and is generally accepted by States." U.N. ExComm Conclusion No. 6 (XXVIII) Non-Refoulement (28th Sess.) ¶ (a) (1977). In 1981 ExComm concluded, in the context of a "large-scale influx," that "[i]n all cases the fundamental principle of non-refoulement including non-rejection at the frontier-must be scrupulously observed." U.N. ExComm Conclusion No. 22 (XXXII) Protection of Asylum-Seekers in Situations of Large Scale Influx (32d Sess.) ¶ II(A)2 (1981). By 1982 ExComm stated that the principle of non-refoulement ". . . was progressively acquiring the character of a peremptory rule of international law." U.N. ExComm Conclusion No. 25 (XXXIII) General (33d Sess.) ¶ (b). (1982).

97. Vienna Convention on the Law of Treaties art. 38, Jan. 27, 1980, 1155 U.N.T.S. 331 ("Nothing in articles 34 to 37 precludes a rule set forth in a treaty from becoming binding upon a third State as a customary rule of international law, recognized as such.").

98. *Id.*, art. 64 ("If a new peremptory norm of general international law emerges, any existing treaty which is in conflict with that norm becomes void and terminates.").

99. Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1984 I.C.J. 392, ¶ 73 (Nov. 26); Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶¶ 174–79 (July 27); North Sea Continental Shelf Cases (F.R.G./Den.; F.R.G./Neth.), 1969 I.C.J. 3, ¶¶ 64, 70–74 (Feb. 20).

100. IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 8–10 (7th ed. 2008).

component."[101] Significantly, these calculations include the wide variety of conventions such as the European Convention on Human Rights[102], the OAU Refugee Convention,[103] the American Convention on Human Rights[104] and the Banjul Charter[105] that make provision for *non-refoulement* (either explicitly or as interpreted) outside the strict definition of refugee in the 1951 Refugee Convention and in respect of torture and threats to life.

As such,

> the evidence points overwhelmingly to a broad formulation of the prohibition as including torture or cruel, inhuman or degrading treatment or punishment. With the exception of the Torture Convention, these elements all appear in human rights instruments of both a binding and a non-binding nature as features of a single prohibition.[106]

So, and in parallel to the right of *non-refoulement* as found in both the ICCPR and CAT, the customary norm does not require a causal nexus to be established between the ill-treatment feared and the motivations of the persecuting actor. Correspondingly, the customary right is considerably broader than the right of *non-refoulement* found in Article 33 of the 1951 Refugee Convention. This is significant in the present case as it appears that both the right to protection against torture,[107] and *non-refoulement* more generally,[108] have now attained the status of preemptory/*ius cogens* norms of

---

101. Sir Elihu Lauterpacht and Daniel Bethlehem, *The Scope and Content of the Principle of Non-Refoulement: Opinion*, *in* REFUGEE PROTECTION IN INTERNATIONAL LAW: UNHCR'S GLOBAL CONSULTATIONS ON INTERNATIONAL PROTECTION 87, 147 (Erika Feller, Volker Türk & Frances Nicholson eds., 2003).

102. ECHR, *supra* note 53.

103. OAU Refugee Convention, *supra* note 75.

104. American Convention on Human Rights, O.A. S. Treaty Series No. 36, 1144 U.N.T.S. 123, OEA/Ser.L/V/II.23, doc. 21 rev. 2 (July 18, 1978).

105. Organization of African Unity, African [Banjul] Charter on Human and Peoples' Rights, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982) (entered into force Oct. 21, 1986).

106. Lauterpacht and Bethlehem, *supra* note 103, at 152.

107. Al-Adsani v. United Kingdom (No.2), ¶ 61, App. No. 35763/97, Eur. Ct. H.R. (2001); Prosecutor v. Anto Furundzija, Case No. IT-95-17/1-T, ¶¶ 155–57 (Int'l Crim. Trib. for the Former Yugoslavia Dec. 10, 1998). Erica De Wet, *The Prohibition of Torture as an International Norm of Jus Cogens and Its Implications for National and Customary Law*, 15(1) EUROPEAN JOURNAL OF INTERNATIONAL LAW 97 (2004).

108. U.N. ExComm Conclusion No. 79 (XLVII) General (47th Sess.) ¶ (i) (1996) ("the principle of non-refoulement is not subject to derogation."); U.N. ExComm Con-

public international law. In addition to being generally applicable as norms of customary international law, these are also now supervening norms to which no derogation is permitted.

VI. INTERNATIONAL HUMANITARIAN LAW

A. An International Armed Conflict

There is one further resource for the protection of persons displaced from Syria, which although somewhat more remote from conventional human rights and refugee discourse, must also be taken into account. Both the Third[109] and Fourth[110] Geneva Conventions contain explicit prohibitions of *refoulement*. All of the five key receiving countries are parties to all four Geneva Conventions.[111] In addition, all four conventions are now widely accepted to have passed in their entirety into customary international law.[112] Article 12 of the Third Geneva Convention provides in part that,

> Prisoners of war may only be transferred by the Detaining Power to a Power which is a party to the Convention and after the Detaining Power has satisfied itself of the willingness and ability of such transferee Power to apply the Convention . . . .[113]

Article 45 of the Fourth Geneva Convention provides that,

> Protected persons shall not be transferred to a Power which is not a party to the Convention . . . .

---

clusion No. 25, *supra* note 98, ¶ (b); Jean Allain, *The Ius Cogens Nature of Non-Refoulement* 13(4) INTERNATIONAL JOURNAL OF REFUGEE LAW 533 (2001).

109. Geneva Convention Relative to the Treatment of Prisoners of War, Oct. 21, 1950, 75 U.N.T.S. 135 [hereinafter Third Geneva Convention].

110. Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Oct. 21, 1950, 75 U.N.T.S. 287 [hereinafter Fourth Geneva Convention].

111. A complete list of the State parties to the main international humanitarian law treaties is maintained by the ICRC and may be found at, http://www.icrc.org/ihl/%28SPF%29/party_main_treaties/$File/IHL_and_other_related_Treaties.pdf (last visited Oct. 1, 2013).

112. David Turns, *The Law of Armed Conflict (International Humanitarian Law)*, *in* INTERNATIONAL LAW 814, 816 (Malcom D. Evans ed., 3d ed. 2010); Partial Award on Prisoners of War, Eritrea's Claim (Eri. v. Eth.) 42 I.L.M. 1056, 1083 (Eri.-Eth. Claims Comm'n 2003).

113. Third Geneva Convention, *supra* note 111, art. 12.

> Protected persons may be transferred by the Detaining Power only to a Power which is a party to the present Convention and after the Detaining Power has satisfied itself of the willingness and ability of such transferee Power to apply the present Convention . . . .
>
> In no circumstances shall a protected person be transferred to a country where he or she may have reason to fear persecution for his or her political opinions or religious beliefs . . . .[114]

While Article 12 of the Third Geneva Convention applies only to prisoners of war,[115] Article 45 of the Fourth Geneva Convention applies to State party nationals that find themselves under the control of either a "party to the conflict or occupying power of which they are not nationals."[116] As distinct from the more limited guarantees against *refoulement* found in general asylum and human rights law, the protections in these articles extend to all situations in which the transferee power is *not willing and able to apply the terms of the conventions as a whole*. Furthermore, in respect of the Fourth Geneva Convention only, the protections apply to situations in which the protected person might have reason to fear persecution on political or religious grounds. This last provision thus serves to import a condition similar to the "nexus requirement" in international refugee law.[117]

Of course, the terms of Geneva Conventions III and IV, with the exception of Common Article 3, apply only in the context of an international armed conflict or following a "partial or total occupation of the territory of a High Contracting Party. . . ."[118] There is no suggestion that Syria or, indeed, any of the five key receiving States, is the subject of either an international armed conflict as defined in Common Article 2 or a continuing oc-

---

114. Fourth Geneva Convention, *supra* note 112, art. 45.

115. Third Geneva Convention, *supra* note 111, art. 4.

116. Fourth Geneva Convention, *supra* note 112, art. 4:

> Persons protected by the Convention are those who, at a given moment and in any manner whatsoever, find themselves, in case of a conflict or occupation, in the hands of a Party to the conflict or Occupying Power of which they are not nationals. Nationals of a State which is not bound by the Convention are not protected by it. Nationals of a neutral State who find themselves in the territory of a belligerent State, and nationals of a co-belligerent State, shall not be regarded as protected persons while the State of which they are nationals has normal diplomatic representation in the State in whose hands they are.

117. See discussion at section II(C).

118. Third Geneva Convention, *supra* note 111, art. 2; Fourth Geneva Convention, *supra* note 112, art. 2.

cupation. However, should, as has been widely discussed in recent months,[119] a foreign State intervene to oppose Syrian government forces, the conflict will become "internationalised" within the meaning of Common Article 2. States that become parties to the conflict will then be bound to apply the *non-refoulement* provisions of the conventions in respect of both POWs and State party nationals under their control.

B. A Non-International Armed Conflict

Common Article 3 applies in the context of a non-international armed conflict[120] and there seems little question that the conflict in Syria has now reached the level of a civil war.[121] Although this Article does not contain an explicit prohibition of *non-refoulement* it does feature a broad variety of guarantees against ill-treatment, including in part,

> (a) violence to life and person, in particular murder of all kinds, mutilation, cruel treatment and torture;
> (b) taking of hostages;
> (c) outrages upon personal dignity, in particular humiliating and degrading treatment[122]

There is an obvious analogy with the breadth of the protections found in Articles 6[123] and 7[124] of the ICCPR as interpreted by the Human Rights Committee in their General Comment 20.[125] Further, the language adopted by each convention with respect to the general duties of State parties is largely identical. Both Article 2 of the ICCPR[126] and Common Article 2 of

119. Mark Landler, *Obama Threatens Force Against Syria* NEW YORK TIMES (Aug. 20, 2013), http://www.nytimes.com/2012/08/21/world/middleeast/obama-threatens-force-against-syria.html?_r=0.

120. Third Geneva Convention, *supra* note 111, art. 3; Fourth Geneva Convention, *supra* note 112, art. 3.

121. ICRC 2012 Annual Report, *supra* note 10.

122. Third Geneva Convention, *supra* note 111, art. 3; Fourth Geneva Convention, *supra* note 112, art. 3.

123. ICCPR, *supra* note 80, art. 6.

124. *Id.*, art. 7.

125. U.N. Human Rights Committee General Comment 20, *supra* note 86, ¶ 9.

126. ICCPR, *supra* note 80, art. 2:

> Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the pre-

the Geneva Conventions[127] require States to "respect and ensure" the rights recognized in each convention. This formula provides the basis for the *non-refoulement* obligation in Articles 6 and 7 of the ICCPR as explained by the Human Rights Committee in their General Comment 31.[128] The ICCPR and Common Article 3 feature absolute and non-derogable prohibitions of torture and ill-treatment and the corollary State duties to "respect and ensure" these rights are found in both documents in similar terms. As such, there is every reason to find an identical *non-refoulement* obligation in respect of Common Article 3.[129] This obligation will apply to all State parties involved in the Syrian conflict.

It is likely that this obligation already applies in respect of Iran. As has been widely reported, the Iranian Quds Force is now actively involved in the Syrian conflict.[130] As a result, a duty of *non-refoulement* according to the terms of Common Article 3 now lies against the Iranian State in respect of any Syrian nationals in their control. The same obligation will arise against other States as a corollary of their military involvement in Syria. As States involve themselves in the on-going military conflict in Syria an obligation of *non-refoulement* will arise in respect of any Syrian nationals in their control.

VII. CONCLUSION

At first blush, there might seem to be inadequate resources for the effective legal protection of Syrians displaced to its surrounding States. Few of the key receiving States are parties to either the 1951 Geneva Convention or the 1967 Protocol and none have a functioning domestic asylum system. Where asylum-seekers are registered and claims are determined, this is generally done by UNHCR staff on the basis of an agreement with the host

---

sent Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

127. Third Geneva Convention, *supra* note 111, art. 1; Fourth Geneva Convention, *supra* note 112, art. 1 ("The High Contracting Parties undertake to respect and to ensure respect for the present Convention in all circumstances.").

128. U.N. Human Rights Committee General Comment 31, *supra* note 86, ¶ 12.

129. Cordula Droege, *Transfers of Detainees: Legal Framework, Non-Refoulement and Contemporary Challenges*, 90 INTERNATIONAL REVIEW OF THE RED CROSS 669, 675 (2008).

130. Dexter Filkins, *The Shadow Commander*, THE NEW YORKER, 42, 44 (Sept. 30, 2013) http://www.newyorker.com/reporting/2013/09/30/130930fa_fact_filkins; *Footage Claims to Show Iranians in Syria*, BBC NEWS (Sept. 15, 2013), http://www.bbc.co.uk/news/world-middle-east-24103801.

State.[131] Although Turkey has now passed a comprehensive asylum law it remains, as of yet, unimplemented.[132] As such, any effect it will have on the domestic protection regime for those fleeing the violence in Syria must remain largely a matter of speculation.

Nevertheless, further examination of the international human rights and humanitarian law related to the principle of *non-refoulement* discloses a series of key resources for the protection of Syrians displaced abroad. This includes the absolute and non-derogable guarantees against ill-treatment found in the CAT and the ICCPR together with the corollary State duty of *non-refoulement* explicit in Article 3 of the CAT and, as interpreted, in Articles 6 and 7 of the ICCPR by the Committee on Human Rights.[133] The explicit guarantees against *non-refoulement* found in Article 12 of the Third Geneva Convention and Article 45 of the Fourth Geneva Convention also provide guarantees. While these provisions will be relevant only to an internationalized armed conflict they deserve particular attention given the continuing prospect of military intervention in Syria against the Assad regime by key Western States.[134]

Immediately relevant, however, is Common Article 3, as interpreted by analogy with the reasoning of the Human Rights Committee in respect of Articles 2, 6 and 7 of the ICCPR, to include the right of *non-refoulement*. All of the key receiving States are parties to the four Geneva Conventions and there is little doubt that Syria is now in a state of non-international armed conflict. Indeed, as the Geneva Conventions have passed as a whole into international customary law, their terms will bind any State that seeks to intervene in the Syrian conflict, regardless of whether they are a party to the conventions.

Taken together, the standards found in general international human rights and humanitarian law provide the foundation for an aggressive campaign of advocacy to both receiving States and those States now exploring prospects for military intervention in Syria. As a result of its military involvement in Syria, Iran is already bound by the *non-refoulement* duties implicit in Common Article 3. Other States must understand that, should they

131. This continues to be the case in Lebanon, see *Global Report 2012: Lebanon*, UNHCR, http://www.refworld.org/docid/51c017e919.html (last visited Oct. 13, 2013).

132. See the discussion in section II(B).

133. See the discussion in section IV.

134. Robert Winnett and Peter Dominiczak, *Pressure on Cameron for New Vote on Syria* Strikes, THE TELEGRAPH (Sept. 1, 2013), http://www.telegraph.co.uk/news/worldnews/middleeast/syria/10279620/Pressure-on-Cameron-for-new-vote-on-Syria-strikes.html .

choose to involve themselves in the Syrian conflict, they will assume a *non-refoulement* obligation pursuant to both conventional and customary international humanitarian law in respect of Syrian nationals under their control. This is in addition to the basic right of *non-refoulement* at international human rights and refugee law.

Of course, any program of advocacy will be more effective when it combines practical assistance with exhortation. Recent violations of the right of *non-refoulement*, although troubling, should not distract attention from the extraordinary continuing burden on key receiving States and the challenges this poses authorities at all levels in delivering assistance and protection to the displaced. It is only common sense that, for States caught in the middle of the Syrian crisis, good advice will be welcomed only when it comes together with a helping hand.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Seeking International Criminal Justice in Syria

Annika Jones

89 INT'L L. STUD. 802 (2013)

Volume 89 2013

Seeking International Criminal Justice in Syria

Annika Jones[*]

I. INTRODUCTION

The report of the United Nations Mission to Investigate Allegations of the Use of Chemical Weapons in the Syrian Arab Republic (U.N. Mission), released in September 2013, confirmed that "chemical weapons have been used in the ongoing conflict between the parties in the Syrian Arab Republic, [as well as] against civilians, including children, on a relatively large scale."[1] In a note accompanying the report, the Secretary-General of the United Nations condemned the use of chemical weapons as "a war crime and grave violation of the 1925 Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare and other relevant rules of customary international law."[2]

Although attention in recent months has focused on the atrocities caused by the use of chemical weapons in Syria, throughout the course of the conflict a much wider range of potentially criminal conduct has taken

* Lecturer in Law, School of Law, University of Exeter.

1. Report of the United Nations Mission to Investigate Allegations of the Use of Chemical Weapons in the Syrian Arab Republic on the Alleged Use of Chemical Weapons in the Ghouta Area of Damascus on 21 August 2013, ¶ 27, A/67/997–S/2013/553 (Sept. 16, 2013).

2. *Id.*, Note by the Secretary-General, ¶ 1.

place. In August 2013, the Independent International Commission of Inquiry on the Syrian Arab Republic reported massacres and unlawful killings, arbitrary arrests and unlawful detention, hostage taking, enforced disappearance, torture and ill-treatment, sexual violence, violation of children's rights, unlawful attacks, attacks on protected persons and objects, pillaging and destruction of property, use of illegal weapons (including chemical weapons), sieges and attacks on food security.[3] The report suggests that a broad array of war crimes and crimes against humanity have been committed on Syrian territory by both government forces and anti-government armed groups.[4]

Individuals responsible for these serious crimes must be held accountable for their actions. International criminal justice plays an important role in responding to the commission of international crimes. The investigation and prosecution of individuals serves a variety of purposes, from retribution to deterrence to establishment of the truth.[5] Perhaps most importantly, the international criminal justice process has been understood to provide a foundation for future peace by breaking down assumptions of collective guilt, creating a basis for reconciliation and preventing calls for revenge.[6]

In the absence of domestic criminal proceedings, the International Criminal Court (ICC), which came into operation in 2002 and has prospective jurisdiction over the most serious crimes of concern to the international community,[7] provides perhaps the most obvious venue to hold accountable those who have committed serious crimes in Syria. Other possible settings include an *ad hoc* international criminal tribunal created under the Chapter VII powers of the United Nations Security Council,[8] an interna-

3. U.N. Gen. Assembly, Human Rights Council, Report of the Independent International Commission of Inquiry on the Syrian Arab Republic, ¶¶ 40–190, U.N. Doc. A/HRC/24/46 (Aug. 16, 2013).

4. *Id.*, ¶¶ 192, 194.

5. For discussion of the purposes of international criminal justice, see Mirjan Damaška, *What is the Point of International Criminal Justice?* 83 CHICAGO-KENT LAW REVIEW 329 (2008); Payam Akhavan, *Can International Criminal Justice Prevent Future Atrocities?*, 95(1) AMERICAN JOURNAL OF INTERNATIONAL LAW 7 (2001); Antonio Cassese, *Reflections on International Criminal Justice* 61 MODERN LAW REVIEW 1 (1998).

6. Cassese, *supra* note 5, at 1, 6, 10.

7. Rome Statute of the International Criminal Court arts. 5, 11, July 17, 1998, 2187 U.N.T.S. 90.

8. *See, e.g.*, Statute of the International Criminal Tribunal for the Former Yugoslavia (ICTY), S.C. Res. 827, U.N. SCOR, 48th Sess., 3217th mtg., U.N. Doc. S/RES/827 (May 25, 1993), adopting The Secretary-General Report Pursuant to Paragraph 2 of Security Council Resolution 808; Statute of the International Criminal Tribunal for Rwanda

tionalized criminal tribunal with domestic and international elements,[9] and the domestic courts of third States operating on the basis of universal jurisdiction. The remainder of this article will examine the possible institutions in which justice may be sought for the crimes committed in Syria. It concludes by emphasizing the benefits of a multi-layered response, combining both domestic and international(ized) institutions.

II. POSSIBLE VENUES FOR JUSTICE

A. Domestic Courts in Syria

Syrian authorities are under an obligation to investigate and prosecute those suspected of having committed international crimes on Syrian territory.[10] This obligation has its basis in both customary and conventional international law.[11] There are several advantages to the pursuit of justice in

(ICTR), S.C. Res. 955, U.N. SCOR, 49th Sess., 3453d mtg., U.N. Doc. S/RES/955 (Nov. 8, 1994).

9. Examples include Statute of the Special Court for Sierra Leone, Jan. 16, 2002, 2178 U.N.T.S. 145; Law on the Establishment of the Extraordinary Chambers in the Courts of Cambodia for the Prosecution of Crimes Committed During the Period of Democratic Kampuchea (2001), amended by NS/RKM/1004/006 (Oct. 27, 2004), *available at* http://www.eccc.gov.kh/sites/default/files/legal-documents/KR_Law_as_amended_27_Oct_2004_Eng.pdf; Law of the Iraqi Higher Criminal Court, No. 10 (Oct. 9, 2005), Official Gazette of the Republic of Iraq, No. 4006 (Oct. 18, 2005); Statute of the Special Tribunal for Lebanon, S.C. Res. 1757, Annex, U.N. Doc. S/RES/1757 (May 30, 2007); War Crimes Chamber of Bosnia and Herzegovina, State Court, Special Department for War Crimes in the State Prosecutor's Office (Mar. 9, 2005), http://www.sudbih.gov.ba/?jezik=e.

10. The obligation on State authorities to prosecute international crimes committed in Syria has been discussed by the Independent International Commission of Inquiry on the Syrian Arab Republic. *See* U.N. Gen. Assembly, Human Rights Council, Report of the Independent International Commission of Inquiry on the Syrian Arab Republic, ¶¶ 21–24, U.N. Doc. A/HRC/21/50 (Aug. 16, 2012).

11. A customary obligation in international and non-international armed conflict has been recognized by the ICRC. CUSTOMARY INTERNATIONAL HUMANITARIAN LAW (2 volumes) r. 158 (Jean-Marie Henckaerts & Louise Doswald-Beck eds., 2005) [hereinafter Customary IHL Study]. An obligation to prosecute in respect of acts of torture can also be found under the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment and Punishment arts. 5, 7, June 26, 1987, 1465 U.N.T.S. 85. The scope of this obligation has recently been discussed by the International Court of Justice. See Questions

the domestic courts of States on whose territory crimes are committed. These include the potential for greater impact within the local population and access to evidence and perpetrators that exceeds that of the other options, all of which rely on State cooperation.

The pursuit of justice at the domestic level in Syria is, however, unlikely while the conflict continues.[12] Even when the conflict ends, domestic courts can be expected to face difficulties overseeing the investigation and prosecution of the complex international crimes that have been committed in their own State. The construction of domestic capacity in the aftermath of the conflict is crucial in light of the limited capacity of international criminal justice institutions, such as the ICC, an internationalized tribunal and third States, to oversee the investigation and prosecution of a large number of cases. The strengthening of domestic criminal justice institutions is necessary to ensure that individuals who cannot be investigated and prosecuted elsewhere do not go unpunished.[13]

B. The International Criminal Court

The ICC is intended to act as a "court of last resort," which operates in the absence of genuine proceedings at the domestic level.[14] Cases are admissible before the ICC if they are not being, and have not been, investigated or prosecuted by a State with jurisdiction, and if they are of sufficient gravity to justify further action by the Court.[15] The ICC provides a possible route to justice in the absence of genuine proceedings at the domestic level. In many respects the ICC is well placed to address the crimes allegedly committed in Syria. The Court is an established institution with the capacity to

---

Relating to the Obligation to Prosecute or Extradite (Belg. v. Sen.), 2012 I.C.J. 144 (July 20).

12. U.N. Gen. Assembly, Human Rights Council, Report of the Independent International Commission of Inquiry on the Syrian Arab Republic, Annex XIV, 22d Sess., U.N. Doc. A/HRC/22/59 (Feb. 5, 2013) [hereinafter Report of the Independent International Commission of Inquiry on the Syrian Arab Republic].

13. *Id.*

14. For discussion of the principle of complementarity, see Carsten Stahn, *Complementarity: A Tale of Two Notions* 19 CRIMINAL LAW FORUM 87 (2008); John. T. Homes, *Complementarity: National Courts versus the ICC*, *in* THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT: A COMMENTARY (Volume II) (Antonio Cassese, Paola Gaeta & John R. W. D. Jones, eds., 2002).

15. Rome Statute, *supra* note 7, art. 17.

investigate and prosecute complex international crimes cases.[16] It is less susceptible to bias than domestic courts and may be less likely to spark further conflict in the region.[17] For this reason, it may provide an appropriate forum for proceedings against higher-level perpetrators that may be more politically charged and destabilizing.

There are, however, a number of difficulties associated with the ICC as a forum for justice in Syria. One key issue is that of triggering the Court's jurisdiction. Since Syria is not a State party to the Rome Statute, a referral from the United Nations Security Council, acting under Chapter VII of the U.N. Charter, is required to trigger the jurisdiction of the Court.[18] A State party to the Rome Statute cannot refer the situation to the ICC; nor can the Prosecutor initiate an investigation *proprio motu*.[19] The Security Council has already made two referrals to the ICC, in relation to the situation in Darfur, Sudan, in 2005 and that in Libya in 2011.[20] Whilst some members of the Security Council, including the U.K. and France, have supported the referral of the situation in Syria to the ICC, the U.S., China and Russia, each of which holds the power to veto action by the Security Council, have not supported such a move.[21] Russia is reported to have described a referral as

16. For information on the twenty cases in eight situations that have been brought before the ICC, see *Situations and Cases*, ICC, http://www.icc-cpi.int/en_menus/icc/situations%20and%20cases/Pages/situations%20and%20cases.aspx (last visited Nov. 19, 2013).

17. William W. Burke-White, *A Community of Courts: Toward a System of International Criminal Law Enforcement* 24(1) MICHIGAN JOURNAL OF INTERNATIONAL LAW 1, 15–16 (2002–2003).

18. Rome Statute, *supra* note 7, arts. 12–13.

19. *Id.*

20. *See* S.C. Res. 1593, U.N. Doc. S/RES/1593 (Mar. 31, 2005); S.C. Res. 1970, U.N. Doc. S/RES/1970 (Feb. 26, 2011).

21. Amnesty International has identified 64 countries that support a referral of the situation in Syria to the ICC, including six members of the U.N Security Council. *The Countries that Support Referring Syria to the International Criminal Court—and Some Absent 'Friends'*, AMNESTY INTERNATIONAL UK, http://www2.amnesty.org.uk/blogs/campaigns/syria-icc-international-criminal-court (last visited Nov. 19, 2013). In January 2013, Switzerland, together with the governments of 56 States, including the U.K. and France, requested the Security Council "to act by referring the situation in the Syrian Arab Republic as of March 2011 to the International Criminal Court (ICC) without exceptions and irrespective of the alleged perpetrators." See Letter from the Permanent Mission of Switzerland to the United Nations Security Council Secretariat, Jan. 14, 2013, *available at* http://www.news.admin.ch/NSBSubscriber/message/attachments/29293.pdf.

"ill-timed and counterproductive."[22] Therefore, a referral from the Security Council is, for the time being, unlikely.

It would, of course, be possible for a post-conflict government in Syria to ratify the Rome Statute and refer its own situation to the ICC or permit the Prosecutor to exercise jurisdiction on the basis of her *proprio motu* powers of investigation.[23] The ICC has already received a number of referrals from States concerning crimes committed on their territory.[24] Self-referrals have been criticized as an abdication of responsibility to investigate and prosecute on the part of domestic authorities.[25] However, such referrals are both consistent with the text of the Rome Statute and its object and purpose, which is to ensure that individuals are held accountable for the commission of international crimes in situations where justice is not sought at the domestic level.[26] Another option would be for the Syrian authorities to accept the jurisdiction of the ICC under Article 12(3) of the Rome Statute, which would allow the Prosecutor to initiate an investigation *proprio motu*.[27]

It is important that any future referral from the Security Council or a State party to the Rome Statute does not undermine the independence of the ICC by seeking to limit the scope of the referral to one side of the con-

---

22. *See UPDATE 1-Russia Opposes Syria Crisis War Crimes Referral*, REUTERS (Jan. 15, 2013), http://www.reuters.com/article/2013/01/15/syria-crisis-russia-idUSL6N0AKCNB20130115.

23. Rome Statute, *supra* note 7, art. 13. In order to allow the Court to address crimes committed since the beginning of the conflict the Syrian authorities would need to make a declaration under Article 12(3) accepting the jurisdiction of the Court for crimes committed after entry into force of the Statute in 2002. If no declaration is made, the Court would only have jurisdiction with respect to crimes committed after entry into force of the Rome Statute in Syria. *Id.*, art. 11(2).

24. These are the situations in Uganda, the Democratic Republic of the Congo, the Central African Republic, Mali and, more recently, the Union of the Comoros.

25. WILLIAM A. SCHABAS, THE ROME STATUTE OF THE INTERNATIONAL CRIMINAL COURT 165 (4th ed. 2011). *See also* Phil Clark, *Chasing Cases: The ICC and the Politics of State Referral in the Democratic Republic of the Congo and Uganda*, *in* THE INTERNATIONAL CRIMINAL COURT AND COMPLEMENTARITY: FROM THEORY TO PRACTICE (Volume II) 1201 (Carsten Stahn & Mohamed M. El Zeidy eds., 2011).

26. *See* Darryl Robinson, *The Mysterious Mysteriousness of Complementarity*, 21 CRIMINAL LAW FORUM 67 (2010).

27. An investigation has been initiated in such a manner in the Côte d'Ivoire. *See* Situation in the Côte d'Ivoire, Case No. ICC-02/11-14, Decision Pursuant to Article 15 of the Rome Statute on the Authorization of an Investigation into the situation in the Republic of Côte d'Ivoire, Pre-Trial Chamber III, (Oct. 3, 2011), http://www.icc-cpi.int/iccdocs/doc/doc1240553.pdf.

flict.[28] Where States have attempted to do so in the past, the Prosecutor has interpreted the referral to include all crimes committed within the territory.[29] If the Security Council was to refer one side of a conflict to the ICC, the Prosecutor could refuse to initiate an investigation under Article 53(1)(c) of the Rome Statute, which requires the Prosecutor to determine that an investigation would be in the interests of justice.[30]

Another difficulty raised by prosecutions at the ICC is the Court's reliance on the cooperation of States to oversee the criminal justice process. If the jurisdiction of the Court is triggered and the Prosecutor decides to initiate an investigation, the Court will be heavily dependent on State cooperation to gain access to evidence, transfer perpetrators to the Court, protect witnesses and so on. Past practice has shown that State cooperation has not always been forthcoming in relation to situations that have been referred to the ICC by the Security Council, despite the existence of an obligation to cooperate in the Security Council resolution making the referral.[31] Moreover, whilst a self-referral from Syrian authorities may initially be

28. For discussion as to whether or not the Security Council could restrict a referral to the Syrian government's use of chemical weapons, see Kevin Jon Heller, *Could the Security Council Refer Only Assad's Use of Chemical Weapons?* OPINIO JURIS (Aug. 27, 2013), http://opiniojuris.org/2013/08/27/security-council-refer-assads-use-chemical-weapons/. It should be noted that previous referrals from the Security Council have sought to restrict their scope. *See, e.g.*, S.C. Res. 1970, ¶ 6, U.N. Doc. S/RES/1970 (Feb. 26, 2011) (S.C. Resolution 1970 sought to limit the exercise of the Court's jurisdiction in Libya by providing that "nationals, current or former officials or personnel from a State outside the Libyan Arab Jamahiriya which is not a party to the Rome Statue of the International Criminal Court shall be subject to the exclusive jurisdiction of that State for all alleged acts or omissions arising out of or related to operations in the Libyan Arab Jamahiriya established or authorized by the Council, unless such exclusive jurisdiction has been expressly waived by the State.").

29. Following the Ugandan self-referral in December 2003, the Office of the Prosecutor of the ICC "informed the Government of Uganda that, in compliance with its obligations of impartiality, the Office would interpret the referral to include all crimes committed within Northern Uganda." *See* Office of the Prosecutor, Report on the Activities Performed during the First Three Years (June 2003–June 2006), 25 (Sept. 12, 2006), http://www.icc-cpi.int/NR/rdonlyres/D76A5D89-FB64-47A9-9821-725747378AB2/143680/OTP_3yearreport20060914_English.pdf. However, the Prosecutor has subsequently been criticized for failing to address both sides of the conflict. *See* William A. Schabas, *Complementarity in Practice: Creative Solutions or a Trap for the Court?*, *in* THE INTERNATIONAL CRIMINAL COURT AND NATIONAL JURISDICTIONS 36 (Mauro Politi & Federica Gioia eds., 2008).

30. *See also* Heller, *supra* note 28.

31. *See* Göran Sluiter, *Obtaining Cooperation from Sudan—Where is the Law?* 6 JOURNAL OF INTERNATIONAL CRIMINAL JUSTICE 871 (2008).

accompanied by State cooperation, this could easily be lost following a change in government or the decision of the Prosecutor to investigate the conduct of State officials,[32] rendering the Court ineffective.

A further issue associated with the ICC as a forum for justice concerns the Court's substantive jurisdiction. It is not clear from the text of the Rome Statute whether the Court has jurisdiction to address the use of chemical weapons. Reference to chemical weapons was removed from the Statute during the drafting process as a compromise for States that felt chemical and biological weapons should not be included in the Statute if nuclear weapons were left out.[33] Nevertheless, the Statute was adopted with three provisions that could be read to encompass chemical weapons.[34]

These provisions do not, however, apply to non-international armed conflicts, such as the conflict in Syria.[35] During the first Review Conference of the Rome Statute in 2010, Article 8 was amended to prohibit the use of the same range of weapons in a non-international armed conflict that are not permitted in the context of an international armed conflict.[36] Some ambiguity exists as to the entry into force of the provisions and the ability of the ICC to exercise jurisdiction on the basis of a referral from the Security Council.[37] Putting these issues to one side, the question remains as to

---

32. Paola Gaeta, *Is the Practice of "Self-Referrals" a Sound Start for the ICC?*, 2 JOURNAL OF INTERNATIONAL CRIMINAL JUSTICE 950 (2004).

33. SCHABAS, *supra* note 25, at 138.

34. Rome Statute, *supra* note 7, art. 8(2)(b)(ii) (prohibiting "employing poison or poisoned weapons); *Id.*, art. 8(2)(b)(xviii) (prohibiting "employing asphyxiating, poisonous or other gases, and all analogous liquids, materials or devices"); and *id.*, art. 8(2)(b)(xx) (prohibiting "employing weapons, projections and methods of warfare which are of a nature to cause superfluous injury or unnecessary suffering or which are inherently indiscriminate in violation of the international law of armed conflict . . . .").

35. *See Syria: ICRC and Syrian Arab Red Crescent Maintain Aid Effort Amid Increased Fighting*, ICRC (July 17, 2012), http://www.icrc.org/eng/resources/documents/update/2012/syria-update-2012-07-17.htm.

36. Amendments to the Rome Statute, RC/Res. 5 (2010). *See also* Amal Alamuddin and Philippa Webb, *Expanding Jurisdiction over War Crimes under Article 8 of the ICC Statute*, 8(5) JOURNAL OF INTERNATIONAL CRIMINAL JUSTICE 1219 (2010).

37. The amendment is stated to "enter into force in accordance with article 121, paragraph 5 of the Statute." Amendments to the Rome Statute, *supra* note 36, ¶ 1. It is unclear from the text of Article 121(5) whether the ICC could exercise jurisdiction in relation to the crimes listed in the amendment following referral by the Security Council. For discussion, see Dapo Akande, *Can the ICC Prosecute for Use of Chemical Weapons in Syria?*, EJILTALK! (Aug. 23, 2013), http://www.ejiltalk.org/can-the-icc-prosecute-for-use-of-chemical-weapons-in-syria/.

whether or not the provisions can be interpreted to include the use of chemical weapons.[38]

Another approach would be to bring charges for the war crime of intentionally directing attacks against a civilian population as such or against individual civilians not taking direct part in hostilities.[39] The use of chemical weapons may also constitute a crime against humanity under the Rome Statute if it amounts to a "widespread or systematic attack directed against any civilian population, with knowledge of the attack" and results in one or more of the prohibited acts listed in the Rome Statute, such as murder or torture.[40] It is worth noting that Article 7 of the Rome Statute, which provides the Court with jurisdiction over crimes against humanity, requires the prohibited acts to be carried out "pursuant to or in furtherance of a State or organizational policy to commit such an attack."[41]

Even if the ICC does exercise jurisdiction and gains the State support required to bring perpetrators to justice, it could only ever provide a partial response to the atrocities committed in Syria. The ICC is a court of limited capacity and as such is restricted to trying a small number of perpetrators. If the jurisdiction of the ICC is triggered, the Prosecutor is likely to follow its policy of focusing on those bearing greatest responsibility for crimes committed on the territory,[42] leaving the crimes of lower level perpetrators to be addressed elsewhere.

---

38. For discussion see *id.*; Heller, *supra* note 28.

39. Rome Statute, *supra* note 7, art. 8(2)(e)(i).

40. *Id.*, arts. 7(1)(a) and (f).

41. *Id.*, art. 7(2)(a). In its decision of March 31, 2010, Pre-Trial Chamber II of the ICC interpreted the concept of an organization under Article 7(2)(a) to include non-State entities. *See* Situation in the Republic of Kenya, Case No., ICC-01/09-19, Decision Pursuant to Article 15 of the Rome Statute on the Authorization of an Investigation into the Situation in the Republic of Kenya, Pre-Trial Chamber II, ¶ 92 (Mar. 31, 2010). *See also* Claus Kress, *On the Outer Limits of Crimes against Humanity: The Concept of Organization within the Policy Requirement: Some Reflections on the March 2010 ICC Kenya Decision,* 23 LEIDEN JOURNAL OF INTERNATIONAL LAW 23 (2010).

42. In a policy paper released in 2003, the Office of the Prosecutor stated its policy, in light of the limited resources available to the Court: "On the one hand it will initiate prosecutions of the leaders who bear most responsibility for the crimes. On the other hand it will encourage national prosecutions, where possible, for the lower-ranking perpetrators, or work with the international community to ensure that the offenders are brought to justice by some other means." *See* Office of the Prosecutor, Paper on Some Policy Issues Before the Office of the Prosecutor, International Criminal Court, 3 (Sept. 2003), *available at* http://www.icc-cpi.int/nr/rdonlyres/1fa7c4c6-de5f-42b7-8b25-60aa962ed8b6/143594/030905_policy_paper.pdf.

C. An Ad Hoc International Criminal Tribunal

The formation of an *ad hoc* international criminal tribunal, similar to that created for the Former Yugoslavia and Rwanda under the Security Council's Chapter VII powers, would offer an alternative to prosecution before the ICC.[43] The establishment of an international criminal tribunal for Syria was proposed by a group of U.S. congressmen in September 2013.[44] This approach is questionable for two reasons. First, the creation of such a tribunal would be dependent on the will of the Security Council acting under Chapter VII of the U.N. Charter. It is clear from the refusal of the Security Council to refer the situation in Syria to the ICC that there is currently insufficient will to allow an international criminal justice institution to oversee the investigation and prosecution of crimes committed on the territory.

Second, even if such will did exist, it would be more efficient and cost effective to refer the situation to the ICC rather than to establish another *ad hoc* institution in the image of the International Criminal Tribunal for the former Yugoslavia (ICTY) or the International Criminal Tribunal for Rwanda (ICTR).[45] One of the key benefits of establishing the ICC is that the time-consuming and costly process of creating new institutions can be avoided by referring situations to a permanent mechanism.[46] In the event that sufficient will is gathered for the pursuit of international criminal justice, it would be more likely, and more prudent, for the Security Council to refer the situation to the ICC under Article 13(b) of the Rome Statute than to establish a new institution for the same purpose.

D. An Internationalized Criminal Tribunal

The creation of an internationalized criminal tribunal, combining international and domestic elements in terms of personnel and, perhaps, applica-

---

43. *See supra* note 8.

44. Immediate Establishment of a Syrian War Crimes Tribunal Resolution, H. Con. Res. 51, 113th Cong. (2013) (referred to committee).

45. The total costs of the ICTY and the ICTR have been estimated to be $2,319,357,047 and $1,757,521,910, respectively. *See* Daniel McLaughlin, *International Criminal Tribunals: A Visual Overview,* Report of the Leitner Centre of International Law and Justice (2013), *available at* http://www.leitnercenter.org/files/News/ International%20Criminal%20Tribunals.pdf.

46. Report of the Independent International Commission of Inquiry on the Syrian Arab Republic, *supra* note 12, Annex XIV.

ble law, would provide another possible venue for justice.[47] In August 2013, a group of international experts put forward a proposal for the establishment of such a tribunal.[48] The tribunal would have its seat in Damascus, Syria.[49] Its purpose, according to the proposal, would be to "prosecute those most responsible for atrocity crimes committed in Syria by all sides of the conflict when the political situation permits, presumably following a change in government."[50] The tribunal is envisaged to work alongside the ordinary criminal and military courts of Syria, which would oversee the prosecution of lower level perpetrators. It also could possibly form part of a multilayered institutional arrangement, operating at a midway point between domestic criminal courts and the ICC if a referral is made and the Court's admissibility criteria are satisfied.

The establishment of an internationalized criminal tribunal would provide a possible route to justice in the absence of domestic or international trials. In some respects, trials before an internationalized mechanism may be considered preferable to purely international or domestic trials. One advantage of an internationalized criminal tribunal is its ability to combine international and local personnel. The proposal for an internationalized tribunal for Syria provides that international personnel such as judges or advisers would work alongside domestic staff.[51]

Whilst the involvement of local personnel could enhance the sense of domestic ownership and impact of proceedings within the local population,[52] the participation of international personnel could bring expertise and increase the perceived independence and impartiality of the criminal justice process.[53] The combination of international and domestic personnel could also allow for an exchange of knowledge and expertise which may ultimate-

47. *See supra* note 9.

48. The Draft Statute for a Syrian [Extraordinary] [Special] Tribunal to Prosecute Atrocity Crimes) can be found in the Chautauqua Blueprint for a Statute for a Syrian Extraordinary Tribunal to Prosecute Atrocity Crimes (Aug. 27, 2013), *available at* http://publicinternationallawandpolicygroup.org/wp-content/uploads/2013/09/ Chautauqua-Blueprint1.pdf [hereinafter Chautauqua Blueprint].

49. *Id.*, art. 3.

50. *Id.*, at 1.

51. *Id.*, art. 5.

52. Lindsay Raub, *Positioning Hybrid Trials in International Criminal Justice*, 42 INTERNATIONAL LAW AND POLITICS 1013, 1017, 1041–44 (2009). *See also* Laura A. Dickinson, *The Promise of Hybrid Court* 97 AMERICAN JOURNAL OF INTERNATIONAL LAW 295, 306 (2003).

53. Dickinson, *supra* note 52, at 306.

ly strengthen domestic capacity to oversee the investigation and prosecution of international crimes.[54]

Although the creation of an internationalized criminal tribunal for Syria has many potential advantages, it also raises a number of concerns. One issue is that the involvement of victors in the prosecution of the defeated could result in biased and unfair trials. Other internationalized tribunals, such as the Iraqi High Tribunal and the Extraordinary Chambers in the Courts of Cambodia, have been criticized on this basis.[55] A way of avoiding accusations of victors' justice would be to couple the establishment of an internationalized criminal tribunal with a referral to the ICC.[56] This would allow the ICC to address the most politically sensitive, and possibly destabilizing, cases in an independent and impartial manner and reduce the potential for allegations of bias. It would, of course, be dependent on the will of the post-conflict government (or the Security Council) to make such a referral. Previous tribunals have also faced challenges in the form of financial instability, coordination between their international and national components and difficulties in securing the cooperation of local authorities or the authorities of third States.[57] An internationalized tribunal for Syria could encounter similar obstacles. If it does, the likelihood it will render justice could be significantly reduced.

E. The Domestic Courts of Third States

Individuals responsible for the commission of international crimes in Syria could also be brought to justice before the courts of third States. The principle of universal jurisdiction provides a basis on which States can exercise

54. Raub, *supra* note 52, at 1043; Dickinson, *supra* note 52, at 307.

55. Carsten Stahn, *Syria, Security Resolution 2118 (2013) and Peace versus Justice: Two Steps Forward, One Step Back?*, EJILTALK! (Oct. 3, 2013), http://www.ejiltalk.org/syria-security-resolution-2118-2013-and-peace-versus-justice-two-steps-forward-one-step-back/. In relation to the Iraqi High Tribunal, see Michael A. Newton, *The Iraqi High Criminal Court: Controversy and Contributions*, 88 INTERNATIONAL REVIEW OF THE RED CROSS 862 (2006); Michael P. Scharf, *The Iraqi High Tribunal: A Viable Experiment in International Justice?*, 5(2) JOURNAL OF INTERNATIONAL CRIMINAL JUSTICE 258 (2007); Sylvia de Bertadano, *Were there More Acceptable Alternatives to the Iraqi High Tribunal?*, 5(2) JOURNAL OF INTERNATIONAL CRIMINAL JUSTICE 294 (2007); HUMAN RIGHTS WATCH REPORT, DUJAIL: THE FIRST TRIAL BEFORE THE IRAQI HIGH TRIBUNAL (2006), http://www.hrw.org/reports/2006/11/19/judging-dujail.

56. The operation of hybrid courts has been considered to be compatible with the ICC's complementarity regime. *See* Dickinson, *supra* note 52, at 309.

57. Raub, *supra* note 52, at 1044–46.

criminal jurisdiction over certain offenses despite the lack of a territorial or nationality nexus with the offense.[58] A number of States have used the principle to oversee the prosecution of individuals for the commission of international crimes.[59] Since the principle of universal jurisdiction applies to war crimes and crimes against humanity, it would be applicable to crimes committed on Syrian territory.[60] The exercise of universal jurisdiction by third States may provide a route to justice in the event that domestic courts fail to investigate and prosecute and an international(ized) institution is not given jurisdiction.

It is unlikely, however, that a large number of perpetrators would be tried before the domestic courts of third States. First, a third State must have enacted domestic laws enabling it to investigate and prosecute on the basis of universal jurisdiction.[61] Second, the third State would need to be in possession of sufficient evidence and have access to witnesses before it could carry out a successful prosecution.[62] This would entail the cooperation of the territorial State, which may not be forthcoming. Third, the domestic law of the third State may require presence of the accused on the territory for jurisdiction to be exercised.[63] Even if trials *in absentia* are permitted under its domestic law, such trials are likely to be criticized on human rights grounds.[64] Moreover, difficulties can be expected in gaining access to evidence if the reason for the absence of the accused is connected to refusal of the territorial State to permit extradition.[65] Finally, as affirmed by the I.C.J. in the *Arrest Warrant Case,* sitting government officials are immune from prosecution in the courts of third States during their term of

58. STEVEN R. RATNER, JASON S. ABRAMS & JAMES L. BISHOFF, ACCOUNTABILITY FOR HUMAN RIGHTS IN INTERNATIONAL LAW: BEYOND THE NUREMBERG LEGACY 178 (3d ed. 2009).

59. *Id.*, at 198.

60. *See* Institute of Int'l Law, Seventh Comm'n Resolution, Universal Criminal Jurisdiction with Regard to the Crime of Genocide, Crimes Against Humanity and War Crimes (Aug. 26, 2005) (by Christian Tomuschat), *available at* http://www.idi-iil.org/idiE/resolutionsE/2005_kra_03_en.pdf.

61. RATNER, ABRAMS & BISHOFF, *supra* note 58, at 198.

62. Report of the Independent International Commission of Inquiry on the Syrian Arab Republic, *supra* note 12, Annex XIV.

63. ANTONIO CASSESE, PAOLA GAETA, LAUREL BAIG, MARY FAN, CHRISTOPHER GOSNELL & ALEX WHITING, CASSESE'S INTERNATIONAL CRIMINAL LAW 278 (3d ed. 2013).

64. *Id.*, at 280.

65. *Id.*

office.[66] Consequently, whilst it is possible for third States to prosecute individuals for crimes committed during the conflict in Syria, other mechanisms are likely to play a more significant role in the fight against impunity.

III. CONCLUDING OBSERVATIONS

Justice for the crimes committed during the course of the conflict in Syria is likely to be pursued in a number of different arenas.[67] A combination of accountability mechanisms may, indeed, be desirable. There are clear benefits to the prosecution of higher-level perpetrators before the ICC and an internationalized criminal tribunal, whilst lower level perpetrators are addressed by domestic criminal courts. A multi-layered institutional arrangement would allow the benefits of local trials to be realized and at the same time ensure that the highest level perpetrators are tried fairly and impartially before an international mechanism in a manner that is less likely to disrupt a fragile peace settlement. The potential for several judicial mechanisms to exercise jurisdiction in relation to the crimes committed in Syria raises interesting questions about the nature of the institutional relationship between those mechanisms and the distribution of cases between them.

Regardless of whether or not the situation in Syria is referred to the ICC or an internationalized court is established, domestic courts will have an important role to play in the fight against impunity for crimes committed throughout the course of the conflict. Practice to date has shown that international and internationalized mechanisms are only able to oversee the trial of a relatively small number of high-level perpetrators and would be unable to address all the crimes that are understood to have been committed on Syrian territory. Thought must, therefore, be given to the construction of domestic capacity to investigate and prosecute international crimes as part of the post-conflict reconstruction process.

It is possible for international and internationalized criminal justice mechanisms to play a role in boosting the capacity of domestic criminal courts through the exchange of information and expertise. The impact of

66. Case Concerning the Arrest Warrant of 11 April 2000 (Dem. Rep. Congo v. Belg.), 2002 I.C.J. 3 ¶ 58 (Feb. 14). *See also* RATNER, ABRAMS & BISHOFF, *supra* note 58, at 207.

67. *See* Report of the Independent International Commission of Inquiry on the Syrian Arab Republic, *supra* note 12, Annex XIV.

an internationalized criminal tribunal on the construction of domestic capacity would depend on the nature and degree of interaction between international and domestic staff and efforts made to transfer expertise to local courts. The ICC could also assist in the construction of domestic capacity. Indeed, the principle of complementarity that underpins the ICC's system of justice has been understood to include a "positive" aspect whereby the Court seeks to promote trials at the domestic level.[68] The ways in which the ICC can boost domestic capacity are, however, limited by the budget of the ICC as well as its judicial mandate.[69]

Given the budgetary restrictions of international and internationalized courts and tribunals, and their limited mandates, other international organizations, civil society and third States will be required to contribute in order to build a domestic system capable of seeking justice for those affected by the crimes committed during the course of the conflict in Syria. These actors must now work together to ensure that these atrocities do not go unpunished and that those responsible are brought, fairly and impartially, to justice.

68. Stahn, *supra* note 14, at 88. See also William W. Burke-White, *Implementing a Policy of Positive Complementarity in the Rome System of Justice* 19 CRIMINAL LAW FORUM 19 (2008).

69. For an outline of the role that the Office for the Prosecutor can play in encouraging genuine national proceedings, see The Office of the Prosecutor, International Criminal Court, Prosecutorial Strategy (2009-2012), ¶ 17 (Feb. 1, 2010), http://www.icc-cpi.int/NR/rdonlyres/66A8DCDC-3650-4514-AA62-D229D1128F65/281506/OTPProsecutorialStrategy20092013.pdf.

INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

The Seizure of Abu Anas Al-Libi: An International Law Assessment

Gordon Modarai
David O'Connell
Timothy Kelly
James Farrant

89 INT'L L. STUD. 817 (2013)

Volume 89 2013

The Seizure of Abu Anas Al-Libi: An International Law Assessment

Gordon Modarai
David O'Connell
Timothy Kelly
James Farrant[*]

I. INTRODUCTION

On October 5, 2013, United States forces captured and detained Abu Anas Al-Libi in Tripoli, Libya. Al-Libi was, at one time, a senior member of Al-Qaeda with close links to Osama Bin Laden and, according to U.S. Secretary of State John Kerry, was a "legal and appropriate target."[1] Following his capture, Al-Libi was delivered to a U.S. warship, the USS *San Antonio* (LPD 17), and reportedly interrogated.[2] He was transferred to the

* Captain Gordon Modarai, JAGC, U.S. Navy; Commander David O'Connell, U.S. Coast Guard; Lieutenant Colonel Tim Kelly, U.S. Marine Corps; and, Lieutenant Commander James Farrant, Barrister, U.K. Royal Navy are faculty members at the International Law Department, U.S. Naval War College. The views expressed in this article are those of the authors in their personal capacities and do not necessarily represent the views of their governments.

1. *US Commando Raids: Kerry Defends al-Liby Capture*, BBC NEWS AFRICA (Oct. 7, 2013), http://www.bbc.co.uk/news/world-africa-24426033 [hereinafter BBC NEWS AFRICA].

2. Ernesto Londoño and Karen DeYoung, *Libyan Terrorism Suspect Held Aboard Warship is Brought to U.S.*, THE WASHINGTON POST (Oct. 14, 2013) http://www. washing-

U.S. within eight days of his capture. On October 14, 2013, Al-Libi entered not-guilty pleas to charges stemming from the 1998 Al Qaeda bombing campaign against U.S. embassies in East Africa.[3]

This article addresses three issues concerning Al-Libi's capture and detention. Part II examines the bases on which the U.S. might lawfully have crossed the Libyan border to conduct the operation, since incursion by one State into another can amount to a breach of international law.[4] Part III assesses the grounds, under international law, on which the U.S. might lawfully have captured Al-Libi. Part IV addresses the circumstances of Al-Libi's subsequent detention. In conclusion, Part V lists several principles that can inform similar operations in the future.

II. CROSSING THE LIBYAN BORDER

An incursion into another State's territory violates the use of force prohibition in Article 2(4) of the UN Charter, "even if it is not intended to deprive that State of part of its territory and if the invading troops are meant to withdraw immediately after completing a temporary and limited operation . . . ."[5] The authors therefore accept as a starting point that when U.S. forces crossed the Libyan border and captured Al-Libi, the operation amounted to a use of force against Libya. Three circumstances, however, may preclude the wrongfulness of a sovereignty violation where it also amounts to a use of force: Security Council authorization; consent from the territorial State; and, self-defense.[6] The latter two are relevant to the facts surrounding Al-Libi's capture, and will be considered in turn.

---

tonpost.com/world/national-security/libyan-suspect-held-aboard-warship-is-returned-to-us/2013/10/14/4b199f5e-3501-11e3-be86-6aeaa439845b_story.html.

3. Deborah Feyerick and Lateef Mungin, *Alleged al Qaeda Operative Abu Anas Al Libi Pleads Not Guilty*, CNN (Oct. 15, 2013), http://www.cnn.com/2013/10/15/justice/al-libi-case/.

4. S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (Ser. A) No. 10, at 18 (Sept. 7). *See also* Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, Preamble, G.A. Res. 2625 (XXV), U.N. GAOR, 25th Sess., Supp. No. 28, U.N. DOC. A/RES/8082 (Oct. 24, 1970) (asserting that "[t]he principle of sovereign equality of States," and in particular that "[t]he territorial integrity and political independence of the State are inviolable.").

5. Albrect Randelzhofer & Georg Nolte, *Article 2(4)*, *in* THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 200, 216 (Bruno Simma et al. eds., 3d ed. 2012).

6. *See* Michael N. Schmitt, *Extraterritorial Lethal Targeting: Deconstructing the Logic of International Law*, 52 COLUMBIA JOURNAL OF TRANSNATIONAL LAW (forthcoming 2013), *available at* SSRN http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2226359&download

A. Libyan Consent

It is not clear, as a matter of fact, whether Libya consented to the entry and presence of U.S. forces on its territory. The Libyan Government has stated publicly that it did not consent to the U.S. operation, while U.S. officials have said that Libya knew of the operation in advance, and did not object to it.[7] Assuming that the Libyan Government did consent to the presence of U.S. forces on its territory, there are two subsidiary issues: the scope and quality of Libya's consent.[8]

As to scope, the activities undertaken by the actor State's forces must be within the limits of the consent granted by the territorial State.[9] Libyan consent, tacit or otherwise, would need specifically to have authorized the capture operation. Given the conflicting positions of the protagonist governments, it is presently impossible to conclude whether the U.S. action was within the scope of any consent granted by Libya.

With regard to the quality of consent, must the actor-State ensure that the individual giving consent carries his government's authority? The International Court of Justice (I.C.J.) has frequently held that the consent of a State official, even if *ultra vires* under that State's constitutional arrangements, is still sufficient to bind the State.[10] The only exception to this rule is where the domestic incapacity of the State official is known to the other State, or is "manifest."[11] Accordingly, international law permits the U.S. to

---

=yes [hereinafter Schmitt, *Extraterritorial Lethal Targeting*]. The circumstances that might preclude the wrongfulness of a State breaching the territorial sovereignty of another State in cases which do not rise to the level of a "use of force" contrary to the United Nations Charter, Article 2(4) (including necessity, *force majeure*, distress or countermeasures) are not applicable. *See* International Law Commission, Responsibility of States for Internationally Wrongful Acts, G.A. Res. 56/83 annex, arts. 20–25, U.N. Doc. A/RES/56/83 (Dec. 12, 2001) [hereinafter ILC Draft Articles].

7. Michael S. Schmidt, *U.S. Officials Say Libya Approved Commando Raids*, THE NEW YORK TIMES (Oct. 9, 2013), http://www.nytimes.com/2013/10/09/world/africa/us-officials-say-libya-approved-commando-raids.html?_r=0.

8. *See generally* Ashley S. Deeks, *Consent to the Use of Force and International Law Supremacy*, 54 HARVARD INTERNATIONAL LAW JOURNAL 1 (2013) [hereinafter Deeks, *Consent to the Use of Force*].

9. ILC Draft Articles, *supra* note 6, art. 20.

10. *See, e.g.*, Land and Maritime Boundary between Cameroon and Nigeria (Cameroon v. Nigeria: Eq. Guinea intervening), Judgment, 2002 I.C.J. 303, ¶ 265–66 (Oct. 10).

11. *See, e.g.*, Vienna Convention on the Law of Treaties art. 46, May 23, 1969, 1155 U.N.T.S. 331 [hereinafter VCLT].

rely upon the consent of a Libyan representative without having to make further inquiry into his competence.

An additional question is whether consent to an activity is valid when the territorial State would be forbidden from undertaking that same activity because of its domestic law. It is a general principle of international law that a State may not invoke a provision of its domestic law to justify a breach of its international obligations.[12] This means that if Libya granted the U.S. consent to enter its territory and capture Al-Libi, Libya may not now renege on its prior consent on the basis that its domestic law prohibited the undertaken activity.

The conflicting positions of the two governments make it impossible to resolve whether Libya consented to the U.S. operation. The Libyan Government's denial of consent may have been intended to address domestic concerns about the presence of U.S. forces in Libya. It is clear, though, that if Libya provided consent, U.S. forces would be permitted to enter Libya in order to execute this operation. If Libya did not consent to the U.S. operation, then the U.S. would have to rely on self-defense as a lawful basis to breach Libyan sovereignty.

B. Self-Defense

This article makes a distinction in its analysis between the crossing of the Libyan border and the capture of Al-Libi. Self-defense raises a complexity, however, because it might be relied upon by the U.S. in two ways. It could be used to justify only the crossing of Libya's border, leaving the capture of Al-Libi to be based upon other grounds—the law of war, for example. Or, since international law does not restrict the *means* by which a State may defend itself, self-defense could also be a justification for the capture operation.[13] This section therefore includes both aspects of the operation in its self-defense analysis.

---

12. VCLT, *supra* note 11, art. 27; MALCOM N. SHAW, INTERNATIONAL LAW 941 (6th ed. 2008). For a critique of this position, see Deeks, *Consent to the Use of Force*, *supra* note 8. The ILC Draft Articles similarly forbid a "responsible" State from relying on its internal law as a justification for a failure to comply with its obligations under Part Two of the draft. ILC Draft Articles, *supra* note 6, art. 32.

13. Malvina Halberstam, *In Defense of the Supreme Court Decision in Alvarez-Machain*, 86 AMERICAN JOURNAL OF INTERNATIONAL LAW 736, n.5 (1992); Michael J. Glennon, *State-Sponsored Abduction: A Comment on United States v Alvarez-Machain*, 86 AMERICAN JOURNAL OF INTERNATIONAL LAW 746, 749 (1992).

Article 51 of the United Nations Charter, states that "[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations . . . ."[14] There are three possibilities as to what armed attack the U.S. might be responding to, if Al-Libi's capture is to be analyzed under a self-defense paradigm. The first is that the 1998 embassy bombings, in which Al-Libi allegedly played a leading role, may continue to provide a basis for U.S. action in self-defense.[15] The second is that Al-Libi's capture was conducted in the face of a single "imminent" attack against the U.S., which Al-Libi was planning. The third is that Al-Libi, as a member of Al-Qaeda, was engaged in a campaign of attacks.[16]

Under all three justifications, the perpetrator of the armed attack is a non-State actor. With regard to the second and third justifications, the U.S. would be in the position of acting in self-defense in anticipation of an expected armed attack, rather than in response to an ongoing or completed attack. This section will address these non-State actor and anticipation issues, followed by the traditional immediacy, necessity and proportionality requirements of self-defense.

There is dispute as to whether the law of self-defense extends to attacks by non-State actors.[17] The I.C.J. has been unwilling to consider claims of self-defense against non-State actors whose acts were not directly attributable to a State.[18] However, the plain text of Article 51 does not limit the right of self-defense to armed attacks by States. Since the terrorist attacks of September 11, 2001, States have recognized the right of self-

14. U.N. Charter art. 51.

15. This position has been recently advanced in Christian Henderson, *The Extra-territorial Seizure of Individuals under International Law—The Case of al-Liby: Part I*, EJIL: *TALK!* (Nov. 6, 2013), http://www.ejiltalk.org/the-extraterritorial-seizure-of-individuals-under-international-law-the-case-of-al-liby-part-one/#more-9728.

16. Schmitt, *Extraterritorial Lethal Targeting*, *supra* note 6, at 13–14 n.59, suggests that terrorist groups may act like the military forces of a State and conduct campaigns that consist of related but separate operations punctuated with pauses to allow for regrouping, resupply, etc.

17. *See, e.g.*, Daniel Bethlehem, *Principles Relevant to the Scope of a State's Right of Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors*, 106 AMERICAN JOURNAL OF INTERNATIONAL LAW 769 (2012); Randelzhofer & Nolte, *supra* note 5, at 1416–19.

18. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 139 (July 9); Armed Activities in the Congo (Dem. Rep. Congo v. Uganda), 2005 I.C.J. 168, ¶¶ 146–47 (Dec. 19) [hereinafter Armed Activities].

defense in response to "armed attacks" not attributable to a State.[19] For example, United Nations Security Council Resolutions 1368 (2001) and 1373 (2001) clearly reference "self-defense" and "collective self-defense" measures in response to the 9/11 attacks at a time when the international community knew the attacks were perpetrated by a non-State actor. The present authors join many others who regard this debate as largely settled in favor of this latter view. The U.S. also takes this position.[20]

The White House fact sheet on the conduct of extraterritorial operations against non-State actors balances the victim State's right to defend itself and the territorial State's right to sovereignty.[21] Under the concept of sovereignty, a State has the right to protect its borders from incursions, but also has the duty to prevent its territory from being used by others as the launching point for an armed attack against another State. This balanced approach requires the territorial State to be given a reasonable opportunity to suppress the threat originating from its territory before the victim State exercises self-defense, although the notice requirement is not necessary in every case.[22] If the territorial State fails (or would fail) to act, because it is unwilling or unable to meet its external obligations, the victim State may lawfully exercise its right of self-defense, even without notice.[23] There is

---

19. *See* Schmitt, *Extraterritorial Lethal Targeting*, *supra* note 6, at 9; Armed Activities, *supra* note 18, Separate Opinion Judge Simma, ¶ 11.

20. U.S. Department of Justice Draft White Paper, *Lawfulness of a Lethal Operation Directed Against a U.S. Citizen Who is a Senior Operational Leader of Al-Qa'ida or an Associated Force*, 2 (Nov. 8, 2011), http://msnbcmedia.msn.com/i/msnbc/sections/news/020413_DOJ_White_Paper.pdf. *See also* Harold Hongju Koh, Legal Adviser, U.S. Dep't of State, Address at Annual Meeting of the American Society of International Law: The Obama Administration and International Law, (Mar. 25, 2010), http://www.state.gov/s/l/ releases/remarks/139119.htm [hereinafter Koh speech].

21. White House Office of the Press Secretary, Fact Sheet: U.S. Policy Standards and Procedures for the Use of Force in Counterterrorism Operations Outside the United States and Areas of Active Hostilities, May 23, 2013, http://www.whitehouse.gov/the-press-office/2013/05/23/fact-sheet-us-policy-standards-and-procedures-use-force-counterterrorism [hereinafter White House Fact Sheet].

22. *See* Schmitt, *Extraterritorial Lethal Targeting*, *supra* note 6, at 10.

23. White House Fact Sheet, *supra* note 21 (requiring "[a]n assessment that the relevant governmental authorities in the country where the action is contemplated cannot or will not effectively address the threat to U.S. persons."); Abraham D. Sofaer, *Terrorism, the Law, and the National Defense*, 126 MILITARY LAW REVIEW 89, 108 (1989); Ashley S. Deeks, *"Unwilling or Unable": Toward a Normative Framework for Extraterritorial Self-Defense*, 52 VIRGINIA JOURNAL OF INTERNATIONAL LAW 483 (2012) [hereinafter Deeks, *Unwilling or Unable*]. *See also* Philip Alston, U.N. Human Rights Council, Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, ¶ 35, U.N. Doc.

more than a century of State practice that supports this approach.[24] If the U.S. concluded that an armed attack was being (or was about to be) perpetrated by Al-Libi from Libyan territory, then the U.S. would be obliged to notify Libya in order for Libya to halt the attack. However, if the U.S. also concluded that Libya was unwilling or unable to prevent the attack from occurring, or that Al-Libi would be tipped off, then the U.S. could proceed to act in self-defense without notification.

Most States and scholars accept the general concept of anticipatory self-defense, when an armed attack is imminent.[25] However, there is no consensus as to when an armed attack can be said to be imminent.[26] The *Caroline* doctrine permit[s] anticipatory self-defense when the "necessity of self-defense [is] instant, overwhelming, leaving no choice of means, and no moment for deliberation."[27] While some view this standard as limiting self-defense temporally to immediately before an armed attack,[28] such an approach makes little sense in an era when catastrophic terrorist attacks can occur without warning.[29] Accordingly, an alternative approach is the "last feasible window of opportunity" standard.[30] Under this interpretation, a State, instead, may act in self-defense when the attacker is clearly committed to launching an attack, and the victim State would otherwise lose its opportunity to defend itself unless it acted immediately.

A/HRC/14/24/Add. 6 (May 28, 2010) ("A targeted killing conducted by one State in the territory of a second State does not violate the second State's sovereignty if either (a) the second State consents, or (b) the first, targeting, State has a right under international law to use force in self-defence under Article 51 of the UN Charter, because . . . the second State is unwilling or unable to stop armed attacks against the first State launched from its territory.").

24. Deeks, *Unwilling or Unable*, *supra* note 8 at 486.

25. Randelzhofer & Nolte, *supra* note 5, at 1423.

26. *Id.*, at 1421.

27. Letter from Daniel Webster to Lord Ashburton (Aug. 6, 1842), *reprinted in* 2 INTERNATIONAL LAW DIGEST 412 (John Bassett Moore ed., 1906).

28. *See*, DEREK W. BOWETT, SELF-DEFENCE IN INTERNATIONAL LAW 187–92 (1958).

29. Schmitt, *Extraterritorial Lethal Targeting*, *supra* note 6, at 12.

30. Michael N. Schmitt, *Counter-terrorism and the Use of Force in International Law*, 32 ISRAEL YEARBOOK ON HUMAN RIGHTS 53, 110 (2002); U.S. Attorney General Eric Holder, Remarks as prepared for delivery at Northwestern University School of Law, Mar. 5, 2012, *available at* http://www.lawfareblog.com/2012/03/text-of-the-attorney-generals-national-security-speech/ (stating that the criteria for evaluating imminence include "considerations of the relevant window of opportunity to act, the possible harm that missing the window would cause to civilians, and the likelihood of heading off future attacks against the United States.").

In the context of a campaign of attacks, anticipatory self-defense raises the following question. Does a State have to make an independent imminence determination for each potential future attack or is the fact of a campaign of attacks sufficient? Arguably, if a group is clearly mounting a campaign of attacks, self-defense would be permitted and would not independently need to meet the imminence criterion for each individual potential attack.[31] This is certainly the view of the U.S.,[32] and the authors are broadly supportive of this approach.

In the Al-Libi case, the U.S. has not provided any information about whether it expected (or expects) any particular attack from Al Qaeda, or whether Al-Libi's capture averted an attack. Many news agencies report Al Qaeda's involvement in the 2012 attack on the U.S. embassy in Benghazi. On the other hand, President Obama has repeatedly asserted that core Al Qaeda is "on the way to defeat" and that affiliates, such as Al Qaeda in the Arabian Peninsula, lack the capacity for a major strike.[33] Somewhat contrary to these statements, in order for the U.S. operation to be justified under "anticipatory" self-defense, the U.S. would have to believe that Al-Libi's capture was conducted in anticipation of an imminent attack by him against the U.S., or that Al Qaeda is still perpetrating a campaign of attacks in which Al-Libi is involved.

If, however, the U.S. exercised self-defense, not in anticipation of an imminent attack or in response to an ongoing attack(s), but instead in response to an attack which has already occurred, then the U.S.'s use of force must be within a period of time not too remote from the initial armed attack. This immediacy requirement is based on a reasonableness standard in light of the circumstances at the time. In this case, Al-Libi's participation in the U.S. embassy attacks in east Africa occurred in 1998, 15 years prior to his capture. In the authors' view the use of force to effectuate his cap-

---

31. *Schmitt*, *supra* note 6, at 13–14.

32. *See* John O. Brennan, Assistant to the President for Homeland Security and Counterterrorism, Remarks at the Program on Law and Security, Harvard Law School: Strengthening Our Security by Adhering to Our Values and Laws (Sept. 16, 2011), http://www.whitehouse.gov/the-press-office/2011/09/16/remarks-john-o-brennan-strengthening-our-security-adhering-our-values-an; White House Fact Sheet, *supra* note 21.

33. Fred Lucas, *Obama Has Touted Al Qaeda's Demise 32 Times since Benghazi Attack,* CNS NEWS (Nov. 1, 2012), http://cnsnews.com/news/article/obama-touts-al-qaeda-s-demise-32-times-benghazi-attack-0; Carlo Muños, *President: Al Qaeda is "on the way to defeat",* THE HILL (Aug. 7, 2013), http://thehill.com/video/administration/316057-obama-says-al-qaeda-on-way-to-defeat.

ture in 2013, if exclusively based on his participation in the embassy bombings, fails the immediacy criterion of self-defense.

The use of force in every instance of self-defense must be limited to what is necessary and proportionate.[34] Necessity "requires that there be no alternative to the use of force effectively to defeat an attack that is either imminent or underway."[35] Accordingly, an assessment must be undertaken of the prospects of success for alternative courses of action which do not amount to a use of force. Thus, the use of force to capture Al-Libi could satisfy the necessity principle if, for example, cooperative law enforcement measures to arrest and extradite Al-Libi were expected to fail.

Proportionality addresses the quantity of force that a State can use in self-defense, restricting it to only that force required to eliminate the threat or end the attack.[36] Since Al-Libi's capture was a limited incursion into Libyan territory, a use of minimum, non-deadly force, the authors propound that Al-Libi's capture was a proportionate means of eliminating the threat of an armed attack.

In conclusion, the U.S. has not yet sought to use self-defense as a public justification for the operation, and has instead relied upon the assertion of Libyan consent. The consent justification, if factually accurate, is in compliance with international law. No information provided publicly thus far supports the exercise of self-defense.

III. THE CAPTURE OF AL-LIBI

Part II considered the U.S. operation from the perspective of Libyan sovereignty. This Part addresses what grounds in law the U.S. might have had for capturing Al-Libi, irrespective of the sovereignty (or border crossing) issue. International law norms applicable to the capture and subsequent detention of an individual differ dependent upon whether the capturing State is a party to an armed conflict or not. Because the U.S. has repeatedly asserted that it is engaged in a non-international armed conflict (NIAC) with Al Qaeda and affiliated groups, this paradigm will be considered first,

34. *See* Randelzhofer & Nolte, *supra* note 5, at 1425; Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, ¶¶ 176, 194 (June 27); Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, ¶ 41 (July 8); Oil Platforms (Iran v U.S.), 2003 I.C.J. 161, ¶¶ 43, 73–74, 76 (Nov. 6).

35. *See* Schmitt, *Extraterritorial Lethal Targeting*, *supra* note 6, at 11.

36. *Id.*, at 12.

followed by an examination of whether there is any other lawful basis for Al-Libi's capture in the absence of an armed conflict.

A. Capture during a non-international armed conflict

Al-Libi allegedly is or has been a leading and influential member of core Al Qaeda. If true, the existence of a lawful basis for his capture turns on the following: (1) whether the U.S. is in a NIAC with al-Qaeda; (2) the geographical limits to the NIAC, if any; and, (3) the circumstances under which the law of armed conflict permits capture.

The U.S. has justified Al-Libi's capture under the laws of war.[37] The viability of this justification depends in the first place upon the existence of a NIAC between the U.S. and Al Qaeda, which is determined though the broadly accepted test set out in *Prosecutor* v. *Tadić*: "[A] [non-international] armed conflict exists whenever there is . . . protracted armed violence between government authorities and organized armed groups, or between such groups within a State."[38] Since the U.S. Supreme Court's *Hamdan* v. *Rumsfeld* decision, the U.S. has stated that it is a party to a NIAC with Al Qaeda.[39] However, the U.S. position is not universally accepted. Under strict application of the *Tadić* test, some scholars have queried whether or not the U.S. remains in a *de jure* NIAC with Al Qaeda.[40] Indeed, even among the present authors, opinion is divided on this question of fact.

If one accepts that there is a NIAC, then the second issue is the geographic limitations, if any, of the NIAC. Common Article 3 to the 1949 Geneva Conventions, which is applicable to conflicts "not of an international character," anticipated that such conflicts would occur within the confines of a single State.[41] Notwithstanding this intention, today, the

37. *See* BBC NEWS AFRICA, *supra* note 1.

38. Prosecutor v. Tadić, Case No. IT-94-1-AR72, Decision on Defence Motion for Interlocutory Appeal on Jurisdiction, ¶ 70 (Int'l Crim. Trib. for the Former Yugoslavia, Oct. 2, 1995).

39. Koh speech, *supra* note 20.

40. *See, e.g.*, Mary Ellen O'Connell, *When Is a War Not a War? The Myth of the Global War on Terror*, 12 ILSA JOURNAL OF INTERNATIONAL & COMPARATIVE LAW 535 (2005); Kenneth Roth, *The War Against al-Qaeda is Over*, THE WASHINGTON POST (Aug. 2, 2013), http://articles.washingtonpost.com/2013-08-02/opinions/41000898_1_war-powers-perpetual-war-human-rights-watch.

41. Article 3 Common to the Geneva Conventions (Common Article 3) refers to "armed conflict not of an international character occurring *in the territory of one of* the High Contracting Parties." (emphasis added). Geneva Convention (I) for the Amelioration of

Hamdan decision interpretation is widely-accepted by other States and numerous scholars, indicating that a NIAC *need not* be geographically limited to the territory of a single State. This, then, raises the question of whether there are any geographical limitations when a NIAC is not restricted to the territory of a single State.[42]

The U.S. subscribes to a view that a NIAC occurs where the parties are located, even if the parties are located in more than one State.[43] Accordingly, the mere presence of the enemy in a State is sufficient to say that the NIAC is taking place there.[44] Despite this broad interpretation of the geography question, restrictions on action still exist. The presence of the enemy in another State does not provide sufficient grounds, alone, for the actor State to breach the territorial State's sovereignty. Instead, the actor State must still justify the violation of sovereignty on one of the grounds discussed in Part II. While the authors agree that the clarity of the U.S. approach has much to commend it as *lex ferenda*, it does not appear to be reflected in other State responses to U.S. drone strikes against Al Qaeda members beyond the borders of Afghanistan, which is often characterized by vehement opposition to U.S. practice.[45]

---

the Condition of the Wounded and Sick in the Armed Forces in the Field art. 3, Aug. 12, 1949, 75 U.N.T.S. 31; Geneva Convention (II) for the Amelioration of the Condition of the Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea art. 3, Aug. 12, 1949, 75 U.N.T.S. 85; Geneva Convention (III) Relative to the Treatment of Prisoners of War art. 3, Aug. 12, 1949, 75 U.N.T.S. 135; Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War art. 3, Aug. 12, 1949, 75 U.N.T.S. 287.

42. For discussion, see Louise Arimatsu, *Territory, Boundaries and the Law of Armed Conflict*, 12 YEARBOOK OF INTERNATIONAL HUMANITARIAN LAW 157 (2009); Claus Kress, *Some Reflections on the International Legal Framework Governing Transnational Armed Conflict*, 15 JOURNAL OF CONFLICT AND SECURITY LAW 245 (2010); Sasha Radin, *Global Armed Conflict? The Threshold of Extra-Territorial Non-International Armed Conflicts* 89 INTERNATIONAL LAW STUDIES 696 (2013).

43. White House Fact Sheet, *supra* note 21; SANDESH SIVAKUMARAN, THE LAW OF NON-INTERNATIONAL ARMED CONFLICT 250–52 (2012).

44. Although Sivakumaran argues the more remote from the scene of the conflict, the specificities of the law may change, requiring a higher threshold for lethal targeting, for example. SIVAKUMARAN, *supra* note 43, at 251.

45. E.g., a U.K. cabinet minister has recently condemned the U.S. use of drones in Pakistan and Yemen as a means of prosecuting the conflict with Al-Qaeda. *See* Paul Vale, *Barack Obama Lambasted by Cabinet Minister Ed Davey Over Drone Strikes in Pakistan*, THE HUFFINGTON POST (Dec. 2, 2013), http://www.huffingtonpost.co.uk/2013/11/14/ed-davey-barack-obama-drones_n_4277940.html. The new German Government has also stated it considers extraterritorial drone strikes "illegal." *Germany Stops Buying Armed Drones*,

The third question addresses the legal basis for detention in a NIAC. The International Committee of the Red Cross (ICRC) has said that the power to capture and detain "flows from the practice of armed conflict and the logic of international humanitarian law that parties to a conflict may capture persons deemed to pose a serious security threat and that such persons may be interned as long as they continue to pose a threat."[46] This ground for detention is forward looking, in that it seeks to prevent the detainee from committing some future act harmful to the detaining State. While the U.S. has not provided a specific factual basis for Al-Libi's detention beyond the criminal indictment, as long as he retains his status as a high ranking member of Al Qaeda, then arguably, he continues to pose a potentially serious threat to the security of the U.S. and is detainable on this basis. However, this justification would likely have to reconcile other U.S. statements that suggest Al Qaeda, as a whole, is now a spent force on its way to defeat.

Nothing prohibits the U.S. from transferring Al-Libi to the federal criminal justice system, presuming that he was lawfully captured under the law of war. Indeed, international law plainly anticipates that members of organized armed groups in a NIAC may be subjected to the domestic criminal jurisdiction of the State party to the conflict.[47]

B. Alternative Bases for Capture

While many still view the conflict with Al Qaeda as a NIAC, if the situation no longer crosses this threshold, then Al-Libi's capture must be examined

---

THE HUFFINGTON POST (Nov. 14, 2013), http://live.huffingtonpost.com/r/ archive/segment/germany-stops-buying-armed-drones/528520e3fe34444eb1000407.

46. *Expert Meeting on Procedural Safeguards for Security Detention in Non-International Armed Conflict*, 91 INTERNATIONAL REVIEW OF THE RED CROSS 859, 863 (2009). This ground was also implicitly accepted by the group of States that participated in the Copenhagen Process, resulting in a set of non-legally binding principles and guidelines on the handling of detainees in "internationalised internal armed conflict and in peace operations." Copenhagen Process on the Handling of Detainees in International Military Operations, The Copenhagen Process: Principles and Guidelines, ¶ 12 (2012), *available at* http://um.dk/en/~/media/UM/English-site/Documents/Politics-and-diplomacy/Copenhangen%20Process%20Principles%20and%20Guidelines.pdf [hereinafter Copenhagen Principles]. Another author has said detention is a corollary of the power to target individuals during an armed conflict. SIVAKUMARAN *supra* note 43, at 301–02.

47. Common Article 3(1)(d); Protocol Additional to the Geneva Conventions of August 12, 1949, and Relating to the Protection of Victims of Non-international Armed Conflicts art. 6, June 8, 1977, 1125 U.N.T.S. 609 [hereinafter AP II].

under general international law, and not the *lex specialis* of the law of armed conflict. Without reliance on the law of armed conflict, Al-Libi's capture and subsequent detention then would be governed by international law norms regulating the extraterritorial enforcement of a State's domestic jurisdiction and human rights law.[48]

As Part II showed, in the absence of consent of the territorial State, or any other lawful basis in self-defense, Al-Libi's capture would amount to an unlawful infringement of Libyan sovereignty, and an improper extraterritorial enforcement of U.S. domestic criminal jurisdiction. Historically though, an unlawful capture has not provided the criminal defendant with a basis for challenging the State's criminal jurisdiction over him. The principle *male captus bene detentus* provides that "a person improperly seized may nevertheless properly be detained (and brought to trial)."[49]

In *U.S.* v. *Alvarez Machain*,[50] the Supreme Court of the United States held that the seizure of Alvarez-Machain by U.S. agents in Mexico was "shocking" and likely to be "in violation of general international law principles," but did not vitiate the jurisdiction of a U.S. federal court to try him.[51] A similar position was reached by the English Divisional Court in *R* v. *Plymouth Justices, ex parte Driver*.[52] In probably the most famous extraterritorial seizure case of all, the Supreme Court of Israel adopted the same approach in the *Eichmann* case.[53] Contemporary commentators agreed that *male captus bene detentus* is a rule of international law, although many have been critical of it.[54] It must be noted though, that *male captus bene detentus* pre-dates substantial developments in international human rights law.

The European Court of Human Rights (ECtHR), in *Öcalan* v. *Turkey*,[55] recently considered the issue of extraterritorial enforcement from a human rights perspective. Öcalan was wanted in Turkey for offenses related to terrorism. He managed to escape to Kenya, but was later detained by the

48. *See generally* SHAW, *supra* note 12, at 688.

49. Louis Henkin, *International Law: Politics, Values and Functions*, 216 RECUEIL DES COURS 9, 305 (1989).

50. U.S. v. Alvarez Machain 504 U.S. 655 (1992).

51 Alvarez, *supra* note 50, at 669.

52. R v. Plymouth Justices, ex parte Driver [1986] QB 1, at 95 (Eng.).

53. Attorney General of Israel v. Eichmann**,** 36 I.L.R. 5 **(**Dist. Ct. 1962) (Isr); Attorney General of Israel v**.** Eichmann**,** 36 I.L.R. 277 (Sup. Ct. 1962).

54. *See generally*, Halberstam, *supra* note 13; Glennon, *supra* note 13. *See also*, Beth van Schaack, *Al-Liby: Male Captus, Bene Detentus?*, JUST SECURITY (Oct. 7, 2013), http://justsecurity.org/2013/10/07/Al-Libi-male-captus-bene-detentus/.

55. Öcalan v. Turkey, App. No. 46221/99, Eur. Ct. H.R. (2005).

Kenyan authorities in order to return him to Turkey to face trial. The ECtHR held that his transfer to Turkish jurisdiction was conducted with the consent and co-operation of the Kenyan government such that it did not breach Öcalan's human right to freedom from arbitrary detention. However, the ECtHR opined that without Kenyan consent, Turkey would not have had criminal jurisdiction over Öcalan,[56] because an extraterritorial capture would not have been in accordance with a "procedure prescribed by law" within the meaning of Article 5(1) of the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms (or EHCR).[57]

The *Öcalan* decision focused on the interpretation of Article 5 of the ECHR, and so it is plainly not binding on the U.S. But Article 5 of the ECHR and Article 9 of the 1966 International Covenant on Civil and Political Rights (ICCPR)[58] are united in forbidding arrest and detention which is not "in accordance with a procedure prescribed by law." The U.S. has ratified the latter instrument.[59] Although the U.S. does not accept the extraterritorial application of the ICCPR, it does acknowledge that it is globally bound by customary human rights law.[60] Of relevance to the Al-Libi case, the U.S. recognizes that customary human rights law contains a prohibition against arbitrary detention.[61] It is not clear, however, that a U.S. tribunal would interpret the word "arbitrary" to include unlawful extraterritorial arrest as the ECtHR has done.

While many jurisdictions continue to recognize the "*male captus bene detentus*" doctrine, there are contradictory decisions from the same courts which have indicated that in some instances, jurisdiction ought to be de-

56. *Id.*, ¶ 99. Öcalan's argument that there could be no jurisdiction is summarized at *id.*, ¶ 79.

57. *Id.*, ¶¶ 90–97. Convention for the Protection of Human Rights and Fundamental Freedoms art. 5(1), Nov. 4, 1950, 213 U.N.T.S. 222 [hereinafter ECHR].

58. International Covenant on Civil and Political Rights art. 9, G.A. Res. 2200A (XXI), U.N. Doc. A/6316 (Dec. 16, 1966), 999 U.N.T.S. 171 [hereinafter ICCPR].

59. The ratification date (June 8, 1992) is available on the UN Treaty Collection database, http://treaties.un.org/pages/viewdetails.aspx?src=treaty&mtdsg_no=iv-4&chapter=4&lang=en (last visited Dec. 4, 2013).

60. For a summary of the history of the U.S. position regarding the extraterritorial application of human rights law (treaty and customary), see Beth Van Schaack, *United States Report to the UN Human Rights Committee: Lex Specialis and Extraterritoriality*, JUST SECURITY (Oct. 16, 2013), http://justsecurity.org/2013/10/16/united-states-5th-periodic-review/.

61. Restatement of the Law Third: The Foreign Relations Law of the United States § 702 (1987).

clined.[62] It is therefore possible that since the *Alvarez-Machain* decision customary international law has been developing beyond the *male captus bene detentus* principle. Consequently, Al-Libi conceivably could contest U.S. criminal jurisdiction using this potential customary human rights norm as the basis for his challenge.[63] If he did, the likelihood of success would be remote since a court would need to conclude that Al-Libi was not lawfully captured under the law of armed conflict, and that a customary norm has developed beyond *Alvarez-Machain*. The court also would have to grapple with the U.S. Supreme Court's precedence.

IV. AL-LIBI'S SUBSEQUENT DETENTION

This part begins by presuming there is a subsisting NIAC between the U.S. and Al Qaeda and will assess whether Al-Libi's detention is lawful under the law of armed conflict. In a NIAC, once an individual is captured, the law of armed conflict provides the detainee with certain protections. Protections relevant to Al-Libi's case will be explored in the first section of this part, and will address whether the law of armed conflict permits the U.S to detain Al-Libi on board a warship. The *lex specialis* of the law of armed conflict may be relied upon in a NIAC by the detaining State, instead of the narrower constrains on detention found in human rights law.[64] This Part will also consider Al-Libi's case exclusively under human rights norms, in the alternative to a NIAC.

---

62. In the U.S., see United States v. Toscanino, 500 F.2d 267 (2d Cir. 1974); in the U.K., see R v. Horseferry Road Magistrates' Court, ex parte Bennett [1993] 3 WLR 90 (Eng.). For other examples see Glennon, *supra* note 13, at 750, n.22.

63. The concurring opinion of Breyer, J. in Kiobel v. Royal Dutch Petroleum, 133 S.Ct. 1659 (2013) indicates a willingness in the U.S. Supreme Court to allow allegations of extraterritorial breaches of customary human rights law against the U.S. government to be litigated in U.S. federal courts. Although this case was in the context of civil litigation under the Alien Tort Statute, the general principle has obvious potential to read across to questions of criminal jurisdiction.

64. *See, e.g.*, ICCPR, *supra* note 58, art. 9 and ECHR, *supra* note 57, art. 5(2). The former contemplates arrest or detention on the basis of criminal charges only, and the latter sets out a finite list of circumstances in which it is lawful to detain an individual. Both articles require that detention will be "promptly" considered by a judge and subject to periodic judicial review thereafter, whereas the law of armed conflict requires only administrative, rather than judicial, oversight of detention.

A. Detention in a NIAC

The rules governing detention in a NIAC are not as well developed as those in international armed conflict (IAC). Only some of the detention norms designed for IACs are applicable in NIACs.[65] In particular, NIAC treaty law contains a limited set of norms on treatment and an absence of rules governing the procedural guarantees for security detention.

It would not be appropriate to import the full panoply of the IAC rules for detention into a NIAC. As noted by the International Criminal Tribunal for the Former Yugoslavia in the *Tadić* case:

> [t]he emergence of the aforementioned general rules on internal armed conflicts does not imply that internal strife is regulated by general international law in all its aspects. Two particular limitations may be noted: (i) only a number of rules and principles governing international armed conflicts have gradually been extended to apply to internal conflicts; and (ii) this extension has not taken place in the form of a full and mechanical transplant of those rules to internal conflicts; rather, the general essence of those rules, and not the detailed regulation they may contain, has become applicable to internal conflicts.[66]

Instead, Common Article 3 of the 1949 Geneva Conventions serves as a baseline standard for treatment upon capture in a NIAC.

Common Article 3 prohibits the murder, mutilation, cruel treatment, torture, and outrages upon personal dignity of all persons taking no active part in hostilities.[67] It also protects those detained from criminal sentencing without due process, affording "all the judicial guarantees which are recognized as indispensable by civilized peoples."[68] Additional Protocol II to the 1949 Geneva Conventions elaborates further upon the safeguards provided for in Common Article 3.[69] U.S. policy regarding the treatment

---

65. *See, e.g.*, Copenhagen Principles, *supra* note 46. For the ICRC position on what rules should govern detention in NIACs, see Jelena Pejic, *Procedural Principles and Safeguards for Internment / Administrative Detention in Armed Conflict and other Situations of Violence,* 87 INTERNATIONAL REVIEW OF THE RED CROSS 375 (2005).

66. Prosecutor v. Tadić, Case No. IT-94-1-A, Appeals Judgment, ¶ 126 (Int'l Crim. Trib. for the Former Yugoslavia, July 15, 1999). The reference to "internal conflicts" is general accepted to refer to NIACs.

67. Common Article 3(1).

68. Common Article 3(1)(d).

69. AP II, *supra* note 47, arts. 4–6.

of detainees in a NIAC accounts for basic humanitarian protections provided for in both Common Article 3 and Additional Protocol II.[70]

There has been no allegation that the conditions of Al-Libi's detention have failed to comply with the standards set out above. However, some have claimed that the mere detention on a warship, *per se,* is unlawful. Those who have made this allegation point to Geneva Convention III, (GC III), Article 22, which provides that "[p]risoners-of-war may be interned only in premises located *on land* and affording every guarantee of hygiene and healthfulness."[71] However, it is important to highlight that GC III, Article 22, is applicable only in IACs, and cannot automatically be imported to a NIAC. Furthermore, even in an IAC, Article 22's applicability only extends to those who have satisfied the criteria for prisoners of war status. Specifically, in order to achieve prisoner of war status, an individual must come within one of the categories contemplated in GC III, Article 4A. Al-Libi does not fall into any of these categories; nor is the conflict in question an IAC. Article 22 therefore does not apply to his detention.

Others may argue that while Article 22 *per se* does not apply in a NIAC, "the general essence" of the article should be applicable during a NIAC on the basis of *Tadić*.[72] This position is difficult to maintain, however. The most comprehensive legal instrument governing NIACs, which is Additional Protocol II, does not contain a rule equivalent to Article 22.[73] Moreover, the rule is hardly all-encompassing during an IAC; for example, there

---

70. As a non-Party to Additional Protocol II, the United States is not bound by its provisions, but the U.S. Secretary of State has said specifically that the Protocol is reflective of U.S. practice and signaled its intent to seek Senate advice and consent for ratification. Hillary Clinton, Secretary of State, Press Statement: Reaffirming America's Commitment to Humane Treatment of Detainees (Mar. 7, 2011), *available at* http://www.state.gov/secretary/rm/2011/03/157827.htm. *See also* Department of Defense Directive 2310.01E, The Department of Defense Detainee Program ¶ 4.1 (Sept. 5, 2006) (providing that "[a] detainee shall be treated humanely and in accordance with U.S. law, the law of war and applicable U.S. policy.").

71. Emphasis added. *See, e.g.*, Spencer Ackerman, *Libyan al-Qaida Suspect's Detention-at-Sea Raises Geneva Convention Concerns*, THE GUARDIAN (Oct. 8, 2013), http://www.theguardian .com/world/2013/oct/08/us-detention-libya-al-liby-ship.

72. *Tadić* Appeals Judgment, *supra* note 66, ¶ 126.

73. AP II, *supra* note 47, art. 5. Moreover, the AP II Commentary on Article 5 makes no mention that such a rule was even discussed in the drafting of AP II. COMMENTARY ON THE ADDITIONAL PROTOCOLS OF 8 JUNE 1977 TO THE GENEVA CONVENTIONS OF 12 AUGUST 1949*,* ¶¶ 4564–96 (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann eds., 1987).

is no equivalent provision for those detained under Geneva Convention IV (GC IV).

The absolutism of Article 22's prohibition against at-sea detention for prisoners of war has been questioned, even in the context of GC III.[74] For example, the ICRC calls for the "sensible interpretation" of Article 22.[75] This is because historically the article had two motivations. First, during the Second World War prisoners of war had been held in ships in unsanitary and unsafe conditions, in particular by Japan.[76] Second, belligerent ships (*a fortiori* warships) were at significant risk of enemy attack, potentially placing any prisoners in danger. These factors are now of less concern than they were at the time of Article 22's drafting.

In contrast to Second World War shipboard detention, modern ships (particularly an advanced amphibious command platform such as the *USS San Antonio*), which are equipped with more than adequate protections from the extremes of temperature and weather, are able to provide sanitary, hygienic conditions and sufficient food and water. In addition, a U.S. warship at sea provides safe conditions for detention without significant risk of enemy attack in the context of the NIAC between the U.S. and Al Qaeda.

More recently, other States have detained prisoners of war aboard warships in keeping with the ICRC's invitation to read Article 22 sensibly. In some circumstances, detention at sea might even be more humane than detention ashore. During the 1982 Falklands Conflict, Argentina, after bilateral discussions with the U.K., agreed that its prisoners of war could be held at sea aboard British warships.[77] This decision was no doubt reached on the basis that a U.K. warship afforded better protection during the South Atlantic winter than make-shift accommodations ashore on the wind-swept Falkland Islands.

The final objection to shipboard detention may include concern over a detainee's access to impartial humanitarian bodies, such as the ICRC. Common Article 3 expressly provides that such groups may "offer their services." The U.S., as a matter of policy, notifies the ICRC of any deten-

---

74. Gregory P. Noone et. al., *Prisoners of War in the 21st Century: Issues in Modern Warfare* 50 NAVAL LAW REVIEW 1 (2004). For a concise discussion of the basis for Article 22 and flexibility in its application during modern conflicts, see also Peter Margulies, *Al-Libi and Detention at Sea*, LAWFARE (Oct. 10, 2013), http://www.lawfareblog.com/2013/10/Al-Libi-and-detention-at-sea/.

75. Margulies, *supra* note 74.

76. A.J. BARKER, PRISONERS OF WAR (1975).

77. Noone et. al., *supra* note 74.

tions and grants access to detainees in all but exceptional situations.[78] Indeed, Ahmed Abdulkadir Warsame, who was held aboard a warship by the U.S., was visited by the ICRC.[79] Critics of Warsame's detention have posited that shipboard detention risks the perception that the ship represents a "black site" in which unlawful interrogation techniques might be used.[80] However, that has not proven to be the case, either with Warsame or, as far as can be known, Al-Libi. There have been no complaints that either of the shipboard detentions was inhumane, or conducted in violation of the Common Article 3 standards.

It remains to be seen whether prolonged detention at sea may, as a matter of fact, become inhumane and therefore unlawful. Factors which could jeopardize the legitimacy of detention at sea might include duration and the adequacy of medical care (whether generally or in relation to a detainee's specific condition). In addition, extreme weather or sea state for an extended period might also risk rendering conditions inhumane. These matters must be determined by the facts as they exist. Furthermore, there is no indication that detention at sea would present procedural ambiguities (such as length of detention, periodic reviews) beyond those that already pertain to detention on land. There is no *per se* prohibition against detention on a warship in a NIAC.

B. Detention under Human Rights Law

If Al-Libi's detention was not based on the *lex specialis* of the law of armed conflict, it must be examined under the general principles of international law, i.e., human rights law. While human rights law does not prohibit detention at sea as a matter of course,[81] there are several other factors that must be considered.

---

78. U.S. Dep't of Army, Reg. 190–8, Enemy Prisoners of War, Retained Personnel, Civilian Internees and Other Detainees, ¶ 5.1(5) (Oct. 1, 1997).

79. Charles Savage, *U.S. Tests New Approach to Terrorism Cases on Somali Suspect*, THE NEW YORK TIMES (July 6, 2011), http://www.nytimes.com/2011/07/07/world/ africa/07detain.html. One of the authors of this paper was present onboard when Ahmed Abdulkadir Warsame was detained.

80. Tom Parker, *A Dangerous Somali Fudge*, AMNESTY INTERNATIONAL (July 8, 2011) http://blog.amnestyusa.org/us/a-dangerous-somali-fudge/; Spenser Ackerman, *Drift: How this Ship Became a Floating Gitmo*, WIRED (July 6, 2011) http://www.wired.com /dangerroom/2011/07/ floating-gitmo/.

81. The ECtHR has dealt with several cases concerning the detention of pirates and others at sea and has never found that detention at sea is *per se* a breach of any human

The ECHR and ICCPR both state that persons arrested or detained must be brought "promptly" before a judge.[82] This is a requirement that is broadly reflected in human rights instruments and State practice, which could mean it is now reflective of customary human rights law, and therefore, may apply to Al-Libi's detention. In *Öcalan*, the ECtHR held that Turkey breached this rule, as reflected in ECHR, Article 5(3), when Öcalan was not brought before a judge until seven days after his detention.[83] In *Brogan* v. *UK*, a case concerning individuals suspected of terrorism, the court found that a period of four days and six hours without review by a judge amounted to a breach of Article 5(3).[84] However, in *Medvedyev* v. *France*, the court found that 13 days' detention at sea, without judicial oversight, did not breach Article 5(3) because it was not "materially possible" to bring the detainees before a judge any sooner.[85] In this case the circumstances were of pirates captured at sea whose transfer to the territory of the detaining State, France, took 13 days. On arrival, the detainees were put before a judge within a few hours, so that as soon as it was "materially possible" the detaining State had complied with Article 5(3). The flexibility in *Medvedev* is also reflected in several similar U.S. domestic cases.[86]

Human rights law, therefore, does not provide a strict time limit. Instead, circumstances, such as the location of detention and the possibility of judicial oversight, are taken into account in determining when an indi-

---

rights norm. *See, e.g.*, Medvedyev and others v. France, App. No. 3394/03, Eur. Ct. H.R. (2010); Jamaa v. Italy, App. No. 27765/09, Eur. Ct. H.R. (2012).

82. ECHR, *supra* note 57, art. 5(3); ICCPR, *supra* note 58, art. 9(3).

83. *Öcalan*, *supra* note 55, ¶¶ 100–05.

84. Brogan and others v. United Kingdom, ¶ 62, App. No. 11209/84, Eur. Ct. H.R. (1988).

85. *Medvedyev*, *supra* note 81, ¶¶ 127–34,

86. *See*, United States v. Purvis, 768 F.2d 1237 (11th Cir. 1985) (holding that five days between arrest at sea and presentation before a magistrate was not "unreasonable delay" even though, after arrest, the Coast Guard cutter continued its normal law enforcement activities, did not proceed to nearest U.S. port, and stopped for 8 hours to attempt to sink an abandoned vessel); United States v. Greyshock, 719 F. Supp. 927, 932–33 (D. Haw. 1989) (deciding that nine days between arrest at sea and presentation before a magistrate was not "unreasonable delay," and rejecting contention that government should have airlifted defendants to a magistrate or have permitted defendants access to Coast Guard communication equipment to contact a magistrate); United States v. Savchenko, 201 F.R.D. 503 (S.D. Cal. 2001) (whereas 16 days might be deemed unreasonable for the delay in first appearance concerning an arrest at the International Border with Mexico, some 16 miles south of the courthouse, the 16 days is more than reasonable for the transport of the fishing vessel from the high seas approximately 500 nautical miles from Mexico to this district under these facts and circumstances).

vidual must be brought before a judge. None of these cases suggest a special exception for situations of terrorism.[87] If the U.S. can show that Al-Libi was put before a judge in New York as soon as it was "materially possible" this rule will not have been breached.

V. CONCLUSION

The extraterritorial capture of Abu Anas Al-Libi raises questions in international law ranging from the circumstances in which it is legitimate for a State to infringe another State's sovereignty to the specific conditions of detention under both the law of armed conflict and general international law. This article has not been able to draw conclusions on every issue raised due to gaps in the known factual narrative. However, the foregoing analysis does allow for the statement of certain principles which may inform the conduct of future similar operations.

(1) Consent of the territorial State will always be the most straightforward legal basis for what would otherwise be an unlawful infringement of the territorial State's sovereignty. Obtaining consent will not always be possible, however, and so alternative legal bases may need to be considered.

(2) Where the sovereignty infringement rises to the level of a "use of force," as it did in the Al-Libi case, the only other legal basis for crossing the border will be self-defense. As this article has shown, self-defense might be used as a circumstance precluding the wrongfulness of the whole capture operation. However it might also be limited to justifying the infringement of sovereignty, with an alternative legal basis (such as in the law of armed conflict) justifying the capture. In either case, the actor State will need to show that action in self-defense is in response to an "armed attack," imminent or actual. In an operation such as this, conducted against a non-State actor, the actor State needs to be satisfied that the territorial State is either unwilling or unable to prevent the armed attack about to be perpetrated from its soil before it may act in self-defense.

87. This is apparent in the ECtHR's reasoning in *Brogan*, *supra* note 84, ¶¶ 56–61.

(3) The capture part of the operation may be grounded in the law armed conflict applicable in a NIAC where the individual(s) to be captured represent a threat to the security of the actor State. Before a capture is affected under the law of NIAC, the actor State needs to be satisfied that the individual(s) to be captured is within the geographic bounds of that NIAC. If the view that the law follows the parties is representative of international law, then the mere presence of the enemy in the territorial State is sufficient to conclude the NIAC is taking place in that State. Following a capture grounded in the law of armed conflict applicable in a NIAC, a capturing State is entitled to transfer the captured individual into its domestic criminal jurisdiction.

(4) If there is no NIAC ground for capture, then the capture operation must be compliant with general international law norms governing extraterritorial enforcement of domestic criminal law. Historically, where such norms were breached during capture, this did not prevent the capturing State from subjecting the individual in custody to criminal trial. Whether customary human rights law has developed to eclipse or alter this rule is unclear, but in the U.S. the principle *male captus bene detentus* remains, for now, enshrined in the Supreme Court *Alvarez-Machain* decision.

(5) Whether the capture is affected under NIAC law or general international law, there is no norm which prevents *per se* the detention of captured persons at sea, in a warship. NIAC law does require detainees be treated humanely and that international organizations such as the ICRC be granted access in all but extraordinary circumstances. Detention at sea is perfectly able to meet these requirements. Where the capture is governed by general international law, customary human rights law may provide that captured individuals are required to be put "promptly" before a judge as soon as it is "materially possible."