

UNITED STATES
ARMY WAR COLLEGE
PRESS
Carlisle Barracks, PA
STRENGTH—WISDOM

CONFIDENCE-BUILDING IN CYBERSPACE: A COMPARISON OF TERRITORIAL AND WEAPONS-BASED REGIMES

Mary Manjikian

U.S. ARMY WAR COLLEGE
SSI
STRATEGIC STUDIES INSTITUTE

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

The Center for Strategic Leadership and Development contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

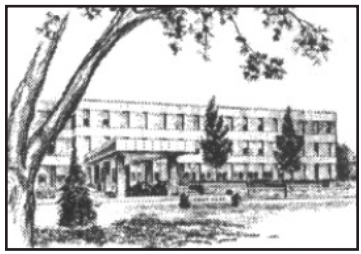
The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.

The Senior Leader Development and Resiliency program supports the United States Army War College's lines of effort to educate strategic leaders and provide well-being education and support by developing self-awareness through leader feedback and leader resiliency.

The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.

The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

STRATEGIC STUDIES INSTITUTE



The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

Strategic Studies Institute
and
U.S. Army War College Press

CONFIDENCE-BUILDING IN CYBERSPACE: A COMPARISON OF TERRITORIAL AND WEAPONS-BASED REGIMES

Mary Manjikian

April 2015

The views expressed in this report are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, the Department of Defense, or the U.S. Government. Authors of Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications enjoy full academic freedom, provided they do not disclose classified information, jeopardize operations security, or misrepresent official U.S. policy. Such academic freedom empowers them to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This report is cleared for public release; distribution is unlimited.

*****

This publication is subject to Title 17, United States Code, Sections 101 and 105. It is in the public domain and may not be copyrighted.

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5010.

*****

This manuscript was funded by the U.S. Army War College External Research Associates Program. Information on this program is available on our website, *www.StrategicStudies Institute.army.mil*, at the Opportunities tab.

*****

All Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press publications may be downloaded free of charge from the SSI website. Hard copies of this report may also be obtained free of charge while supplies last by placing an order on the SSI website. SSI publications may be quoted or reprinted in part or in full with permission and appropriate credit given to the U.S. Army Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, Carlisle, PA. Contact SSI by visiting our website at the following address: *www.StrategicStudiesInstitute.army.mil.*

*****

The Strategic Studies Institute and U.S. Army War College Press publishes a monthly email newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on the SSI website at *www.StrategicStudiesInstitute.army.mil/newsletter.*

ISBN 1-58487-666-2

FOREWORD

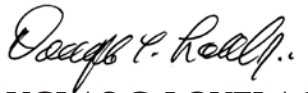
The term "confidence-building measures" is not new. The idea that international actors can come together to share information about their activities in order to establish trust, prevent misunderstandings and misperceptions and de-escalate conflicts is one that has a long pedigree. The development of confidence-building measures in the areas of biological and chemical warfare date back to the beginning of the 20th century. Confidence-building measures aimed at de-escalating conflicts along the Indo-Pakistan border date back to the 1970s.

But what do these diverse events have to offer us as lessons as we think about confidence-building measures in cyberspace? Dr. Mary Manjikian's insightful analysis suggests that both territorially based and weapons-based confidence-building measures can provide models for the ways in which states can learn to cooperate and share information in regard to cyberspace and cyber weapons. We can look at the drive to eliminate biological weapons as a model for the ways in which academics have learned to self-police their research for national security implications, the ways in which they socialize new members of the academic community into the importance of considering security issues, and the ways in which they develop and disseminate norms regarding what is and is not a moral and ethical use of these technologies. Dr. Manjikian recommends that as we move forward as policymakers, we give thought to how academics working on cyber weapons might be similarly motivated to think of themselves as an academic community with norms, procedures, and safeguards. At the same time, we can look at the example of the Indo-Pakistan conflict to see how policymakers have been both suc-

cessful and unsuccessful in creating an environment of relative stability through sharing information about developments along the border with each other. The development of hotlines, reporting requirements, and regular meetings has helped policymakers to establish trust among neighbors though that trust is often fragile and precarious. Here again, this historic example might hold lessons for cyber warriors today, leading to a regime that would include requirements to notify other states when cyber exercises are taking place, to seek information through a hotline before responding in kind, and to activities that bring cyber warriors together on a regular basis to begin to establish trust among all parties.

At the same time, however, these case studies illustrate the challenges that all sides may face in implementing confidence-building measures. They show what happens when not everyone in a regime is equally committed to a specific outcome, they illustrate the difficulties of monitoring compliance in confidence-building regimes, and they show the ways in which doctrines and confidence-building measures may not be perfectly aligned. Again, here we can draw lessons—perhaps about what pitfall to avoid—as we move toward the implementation of confidence-building in cyberspace.

This analysis will give readers much to consider through providing a valuable context in thinking through the implications of confidence-building in cyberspace today.



DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
U.S. Army War College Press

ABOUT THE AUTHOR

MARY MANJIKIAN is Associate Dean of the Robertson School of Government at Regent University. She previously served as a U.S. Foreign Service officer in The Netherlands, Russia, and Bulgaria, and as a Fulbright Scholar at Durham University's Institute of Advanced Study. Dr. Manjikian's publications include *Apocalypse and Post-Politics: The Romance of the End* (Lexington Books, 2012), *Threat Talk: Comparative Politics of Internet Addiction in China and the US* (Ashgate, 2012), and *Securitization of Property Squatting in Western Europe* (Routledge, 2013). Her articles have also appeared in such journals as *International Studies Quarterly*, *International Journal of Intelligence and Counterintelligence*, *Intelligence and National Security*, and the *International Feminist Journal of Politics*. Dr. Manjikian holds an M.Phil. from Oxford Unversity and a Ph.D. from the University of Michigan.

SUMMARY

This monograph examines two historic examples of the development of confidence-building measures (CBMs) so as to make recommendations regarding the development of CBMs for cyberspace. The first study looks at CBMs aimed at preventing the escalation of conflict in contested territories such as the Indo-Pakistan border. The second study looks at the development of a chemical weapons ban following World War I and the establishment of reporting and monitoring procedures to stem the proliferation of chemical weapons. Both cases offer lessons for cyber-based CBMs: One can borrow from territorial CBMs to establish a secure environment, or one can borrow from weapons-based CBMs to shape the development of new cyber technologies and prevent their proliferation.

CONFIDENCE-BUILDING IN CYBERSPACE: A COMPARISON OF TERRITORIAL AND WEAPONS-BASED REGIMES

INTRODUCTION: CONFIDENCE-BUILDING MEASURES IN HISTORIC PERSPECTIVE

As Emily Goldman and John Arquilla have recently noted, the complex and novel nature of cyber technology often makes it difficult for laymen to understand and formulate policy in this field. For that reason it is useful to reason by analogy in order to describe the threats, risks, and opportunities found in cyberspace through borrowing from and seeking comparisons with prior conflicts.[1] Thus far, of course, the most well-known analogy is the description of the risks facing the United States in cyberspace as a result of a surprise attack for which the United States is unprepared to respond, leading to a so-called Cyber Pearl Harbor.

In this analysis, I reason by analogy in presenting two prior situations in which nations have developed confidence-building measures (CBMs) in order to share information and build trust in fields where technology was advancing rapidly and risks were high. In the first case, I describe how the United States worked with allies to bring India and Pakistan to the bargaining table in order to share information and build trust when (physical) border tensions were high. Territorial CBMs aim to build a secure and stable predictable environment through sharing information regarding alleged territorial incursions. In the case of India and Pakistan, this multi-faceted process began in 1947 and is still ongoing, including exchanges of information between both civilians and military personnel. Measures aimed at creating transparency about each side's

activities in territory where borders were unclear, ethnic tensions were great, and the risk of preemptive action by either side was high. If we consider how a security dilemma in real space is addressed when it is difficult to distinguish between offensive and defensive activities, and between preemptive war and offensive war, we can draw insights into how similar dilemmas in cyberspace might be addressed.

In the second case, I examine CBMs in cyberspace through considering, not territory, but instead issues of weaponry. In this analogy, I present the lessons from the Biological Weapons Convention, describing how the scientific-technical and defense communities in the United States worked together to create early warning, monitoring, and verification regimes in order to prevent biological weapons use against civilians and in conflict. Weapons-based CBMs have a different starting point. While territorial CBMs are largely reactive in nature, aimed at containing or de-escalating preexisting conflicts, weapons-based CBMs are preemptive in nature, aimed at socializing weapons producers into working from an agreed-upon set of norms that can shape (or prevent) conflicts that might arise later. What lessons does the Biological Weapons Convention offer cyber policymakers today? In this instance, the scientific-technical community, along with the policy community, established a strong normative regime against the manufacture, use, and deployment of these weapons. Similarly, the cyber community includes both civilian and military manufacturers, producers, and engineers; thus, there are lessons to be learned from the epistemic community of biological weapons scientists. Here the analogy is particularly interesting since the issues of attribution and dual-use are similar between the two types of weapons: biological and cyber.

The decision as to whether current cyber CBMs will be patterned upon territorial or weapons-based CBMs has important implications for the development of a state's overall cyber foreign policy. As Myriam Cavelty has recently argued, current analysts do not agree about what specifically needs to be defended in cyberspace, and they do not appear to be aware of this distinction. However, as she notes, different securitization paradigms tend to stress different referent objects of security.[2]

Thus, choosing the "right metaphor" is not merely important from a literary perspective since the metaphor, in effect, frames the problem. Each metaphor highlights certain aspects of a problem while downplaying others. Furthermore, certain solutions may present themselves clearly, while other less obvious solutions are ignored if the wrong metaphor is chosen. As the comparative case studies in this monograph show, an emphasis on cyberspace as a domain characterized by territorial conflict along borders leads to the conclusion that the military is the most logical actor to take the lead in preventing cyber conflict. On the other hand, descriptions of the weapons used, the danger of proliferation, and the goal of preventing an arms race do not lead to the same conclusion. Instead, an emphasis on weaponry leads to the conclusion that what is needed is export regimes, which are usually controlled and enforced by the Department of Justice and the Department of Commerce. Here, the language of weapons transfers and proliferation of cyber arms is used to describe a criminal problem rather than a security problem for which solutions are criminological rather than military.

In addition, the two metaphors differ in terms of how seriously each portrays the current problem. Military actors concerned with the cyber conflict argue

that the United States has not devoted sufficient funds or energy to combatting this problem, while those concerned with cyber proliferation often feel that current controls are actually too stringent, and that, as a result, they risk harming the competitiveness of U.S. cyber industries on the world market. Similarly, the two types of CBMs protect different things. Territorial CBMs protect cyber territory and objects within that cyber territory (i.e., critical infrastructure) from incursion. In contrast, weapons-based CBMs protect humans and data. The major threat is one of disruption, which could affect the continuity of business interests.[3] Thus, corporate interests are better protected by weapons-based confidence-building measures, and this has increased the "buy-in" of the private sector into the development of CBMs in cyberspace.

In examining the utility of both types of confidence-building measures, it might appear that the decision has already been made—that U.S. and international military planners have already focused on preventing conflict in cyber territory—referring to securing or holding, defending or maintaining one's place in cyberspace.[4] Furthermore, new U.S. and international initiatives to apply the law of armed conflict (LOAC) to events that occur in cyberspace—including borrowing definitions for what it means to launch a preemptive attack or an unprovoked attack, or to violate another state's sovereignty[5]—clearly define cyberspace and CBMs in cyberspace with reference to territory.

However, one can also find reference to combatting the proliferation of cyber weapons, of establishing an international scientific and professional community that would share a consensus about the proper development and use of cyber weapons, and to the ways in which cyber weapons might be codified or modified in order to distinguish between offensive and defensive

cyber weapons. The cyber weapons discourse (versus the cyber territory discourse) more clearly acknowledges the role of nonstate actors in describing cyber weapons as an asymmetric threat, since they can be deployed easily and cheaply by both state and nonstate actors alike.[6]

Figure 1 shows how both types of measures have been proposed for cyberspace.

In point of fact, future CBM provisions for cyber conflict may end up most closely resembling the international arms control regime for nuclear weapons. In that set of protocols, there are both provisions aimed at affecting the activities of scientists who engage in research and development in this area (such as mandating that they carry security clearances and receive proper training on the legislative and ethical restrictions that surround the production and use of these weapons) as well as provisions that describe the ways in which leaders and their teams should react in a crisis situation where nuclear use is suspected. In the first instance, provisions resemble those implemented for weapons-based CBMs, while in the second instance, they resemble provisions implemented for territorial-type CBMs. A further unpacking of both types of CBMs will help to make this point clear.

	Territorial CBM's	Weapons-Based CBM'S
Modeled Upon	• Indo-Pakistan Confidence-Building Measures • Korean Peninsula Confidence-Building measures • Maritime Confidence-Building measures, South China Sea	• United Nations Biological and Toxin Weapons Convention (1975) • United Nations Chemical Weapons Convention (1997) • Australia Group
Actors Involved	• U.S. Cybercommand • Organization on Security and Cooperation in Europe • European Union • Shanghai Cooperation Organization • International Telecommunications Union • Intelligence Community	• United Nations Office of Disarmament and Arms Control • U.S. Department of Commerce • U.S. Department of Justice • Intelligence Community • Nongovernmental Organizations
Values	• Stability within territory • Predictability	• Transparency
Desired End State	• Agreement on Definitions • Application of International law • End misperception, spiral of conflict	• De-escalation of arms raise • End of proliferation • Weapons Ban • Policing by epistemic community
Key Events	Establishment of U.S.-Russian hotline	Wassenaar Arrangement
Proposed Measures	• Limited Force Deployment zones • List of prohibited targets • Hotlines • Advance notification regimes	• Export License Regimes • Verification and Monitoring Regimes • Classification scheme for cyber weapons
Violations Addressed	• Cybertrespass • Dedicated Denial of Service Attacks • Cyberespionage • Preemptive strikes	• Weaponization of code (Malware) • Encryption Issues
How Addressed	International Courts	Domestically through Department of Justice
Current Issues	• Active Defense doctrine incompatible with CBMs? • Is private sector on-board?	• White House lacks commitment to Transparency regarding vulnerabilities • Domestic commitment to making necessary changes in tracking, reporting, prosecuting cyber developments?

Figure 1. A Comparison of Territorial and Weapons Based Confidence-Building Measures for Cyberspace.

CASE STUDY 1: CYBERSPACE AS TERRITORY

Prospects for Applying Territorially Based Confidence-Building Measures.

The application of a territorial metaphor to describe cyberspace is almost as old as cyberspace itself.[7] The language of territoriality can indeed be traced all the way back to the original architects of cyberspace. We can, for example, consider John Perry Barlow's "Declaration of Independence of Cyberspace," which referred to the Internet as a "global social space." While Barlow referred to cyberspace as a sort of global commons, which was unowned and ungoverned,[8] by 2003, the U.S. *National Security Strategy* described the concept of "American cyberspace," taking for granted the notion that cyberspace (or cyber territory) could be both controlled and owned by a particular national entity, and that incursions into a nation's cyber territory could be seen as a threat that required the development of both defensive and offensive strategies in response. Here the U.S. military in particular has been a key actor in putting forth a narrative in which cyberspace is to be treated as territory and as a domain for warfare similar to other domains such as air, land, sea, and space.[9] The 2007 Shanghai Cooperation Organization Action Plan (to which China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, and Uzbekistan are signatories) similarly includes language that stresses that each partner maintains national control over its own Internet.[10]

However, despite emerging understandings that cyber territory was sovereign and should be governed autonomously, we can also trace the expression of sentiments in favor of developing some international

norms regarding state conduct in cyberspace based on the assumption that it was a commons, dating back as early as 2003. In that year, Richard Clarke, a former Special Advisor to the President for Cybersecurity, stated that "having some effective limits on what nations actually do with their cyber war knowledge might, given our asymmetrical vulnerabilities, be in the U.S. national interest."[11] More recently, in a report to the Council on Foreign Relations, former Director of National Intelligence John Negroponte has described the need for a "digital foreign policy," which would include having the United States work with international organizations like the International Telecommunications Union (ITU) to make cyberspace less divided, chaotic, and anarchic.[12]

However, because the borders of territories in cyberspace are often amorphous and because consensus often does not exist regarding where one country's cyberspace begins and another's ends, policymakers can borrow ideas about containing and preempting conflict in cyberspace from the field of territorial CBMs. In both real territory and in cyber territory,[13] one can consider the fact that territories may not be tightly controlled at every point, and that, as a result, vulnerabilities or weaknesses in defense may occur. Abraham Sofaer, David Clark, and Whitfield Diffie refer to such weaknesses or vulnerabilities as sources of cyber insecurity, noting that they may result from flaws and weaknesses in both hardware and software.[14] In particular, we might look to the measures that states have created to attempt to contain and de-escalate conflicts that occur about territorial disputes in areas where borders are amorphous or unclear, such as in maritime areas or in outer space.

In this analysis, I consider the ways in which confidence-building measures have been developed and deployed in preventing border disputes from escalating along the Indo-Pakistan border. In later works, one might also wish to examine confidence-building measures that exist for preventing misunderstandings from occurring in maritime areas.

Defining Territorially Based Confidence-Building Measures.

In considering the use of confidence-building measures in relation to territorial disputes, CBMs are described as measures taken to enable the threshold of animosity between two adversarial nations in order to lower the degree of mutual distrust.[15] A. Z. Hilali describes confidence-building measures as:

> Practical actions aimed at creating attitudes of cooperation; instruments for the prevention of war and conflict and for the resolution of existing conflicts between regional neighbors or parties to the kind of long-standing confrontation, exemplified by the cold war, in which normal channels of communication are weak or have broken down.[16]

Anne Finger and Oliver Meier describe them as an interim step that is less legally binding than a formal agreement that might come later.[17] As an interim step, CBMs do not therefore seek to solve or eliminate the security dilemma. Their chief "product" is thus often not legislation but dialogue, and the process is as important as the end product. Confidence-building measures bring adversaries to the table and engage them in conversations in order to decrease mistrust and create common grounds for future agreements.[18]

Territorial CBMs are often bilateral and may occur between nations that have a long-standing adversarial relationship due to nationalist disagreements; religious, ideological or cultural disagreements; or simply historical events.

In the case of India and Pakistan, the Indian subcontinent was subdivided in 1947 through the establishment of the so-called Radcliffe Line.[19] After Mahatma Gandhi's successful movement for Indian independence, the British withdrew from the region, and new territorial lines were drawn that separated majority Muslim regions from majority Hindu regions. The British withdrawal represented the end of rule by a powerful outside entity with the strength to prevent interethnic conflicts by means of force. Instead, the territorial inhabitants were forced to come to an uneasy truce in a region where borders were new rather than historic, artificially imposed on the region and prone to instability and conflict.[20] Furthermore, there was no regional hegemon able to enforce a truce.



Map 1. The Partition of India and Pakistan, 1947.

Here the parallel with cyberspace is clear. Since the early-1970s when the Internet was a utility developed by the Defense Advanced Research Projects Agency for use only by U.S. military personnel, the "land" of the Internet has become a sort of global territory, accessible to all, where the borders are unclear and subject to change. Furthermore, over time, international actors such as the Internet Corporation for Assigned Names and Numbers have helped to "partition" the Internet through assigning national addresses to various territories or neighborhoods on the Internet. However, as is the case with India and Pakistan, these territorial divisions are clearly artificial, imposed by an outside actor and subject to change. As is the case with India and Pakistan, border clashes and incursions have quickly become a problem requiring solutions in order to prevent a spiral of escalation and violence.

Territorial confidence-building measures rest on the realist assumption that the international system is anarchic, that states act to preserve their own interests, and that in an anarchic system where cooperation is not the rule but the exception, the conditions are set for a security dilemma and a spiral of misperception. States agreeing to confidence-building measures do not do so, therefore, out of an innate desire to cooperate with their neighbors but rather because they rationally have decided that opting out of confidence-building measures presents a greater threat to their own survival and state security.

Here the threat that each seeks to defuse is not only that player A might misunderstand the activities and intentions of player B, but also that both players might misunderstand the activities of some third party (such as a nonstate actor or civilian) who enters the territory and begins to carry out activities. In descriptions of

maritime agreements in the South China Sea, parties to the treaty have voiced concerns that local fisherman might accidentally traverse a boundary as they pursue a school of fish,[21] while officials concerned with cyber trespass have voiced concerns over a scenario where private sector commercial actors might "attack back," targeting computer equipment in a foreign territory in retaliation for attacks against their own systems.[22] In each case, if tensions are already high, such actions easily could be misinterpreted as being sanctioned by state actors.

The specific confidence-building measures adopted between India and Pakistan that have relevance to the diffusion of territorial disputes in cyberspace include the 1987 decision establishing a hotline between political or military leaders of both nations so that in a perceived territorial incursion situation, information can be quickly shared and the situation de-escalated. In addition, in 1988, both parties jointly established a list of facilities that would be off limits for targeting in the event of an outbreak of hostilities, including nuclear facilities. Finally, in 1991, both sides agreed to institute an advance notice requirement regarding the conduct of military exercises along a border or in a border region so that such exercises are not perceived as a military advance.

Figure 2 illustrates the range of military confidence-building measures that have been undertaken in seeking to prevent violence and misunderstandings between India and Pakistan, as well as the events that have occurred that set back confidence-building measures over that time frame.

Timeline: Confidence-Building Measures in Indo-Pakistan Conflict

1947: First Kashmir War

1948: UN negotiates ceasefire, which went into effect in 1949.

1965: War between India and Pakistan ended through Tashkent Declaration (involvement of Soviet Union in peace talks). Both sides agreed to a policy of noninterference in the affairs of each other.

1971: War between India and Pakistan, settled by 1972 Simla Agreement. Both sides agreed not to use force to settle their disputes. Both sides agreed to a bilateral dialogue process for dispute resolution.

1987: Establishment of hotline between Indian and Pakistani Prime Ministers.

1988: First nuclear CBM: agreement not to attack one another's nuclear facilities (ratified 1991, implemented 1992). Agreement to exchange lists of nuclear facilities.

1990: Establishment of a direct communications link between both nations' Directors General of Military Operations, agreement for weekly discussions via the hotline.

1991: Agreement to inform the other side prior to conducting military exercises involving two or more armed divisions in specific areas.

1991: Agreement on non-violation of air space: Neither side's fighter aircraft can enter within 10 kilometers of foreign space.

1992: Accord on prevention of chemical weapons: both sides agreed not to produce, develop or acquire chemical weapons.

Figure 2. A Timeline of CBMs in the Indo-Pakistan Conflict.

1994: Breakdown of talks after India alleged that Pakistan had sponsored terrorism in India.

1997: Resumption of Composite Dialogue between India and Pakistan.

1999: Kargil War, followed by Lahore Declaration: Agreement to upgrade military hotline

2000: Failed Agra Summit.

2001: Attack on India's Parliament, mobilization of troops along border.

2003: Ceasefire between India and Pakistan.

2004: South Asian Association for Regional Cooperation Summit, Islamabad. Pakistan's prime minster assures India that he will not support terrorism against India.

2008: Standoff between two nations related to 2008 Mumbai attacks.

2011: India-Pakistan border shooting.

January 2013: Suspension of Composite Dialogue Process.

Source: Information is From Smruti Pattanaik and Arpita Anant, "Cross-LoC Confidence Building Measures between India and Pakistan: A Giant Leap or a Small Step towards Peace?" New Delhi, India: Institute for Defense Studies and Analyses, February 12, 2010, available from *www.idsa.in/issuebrief/Cross-LoCCBMbetweenIndiaandPakistan_120210*, accessed May 12, 2014. Other sources consulted include T. Najmudheen and Farhana Kausar, "Importance of Confidence Building Measures in India-Pakistan Relationships: A South Asian Perspective," *Asia-Pacific Journal of Social Sciences*, Vol. 5, No. 1, 2013, pp. 61-91.

Figure 2. A Timeline of CBMs in the Indo-Pakistan Conflict. (cont.)

Evaluating the Effectiveness of Territorially Based Confidence-Building Measures.

As is obvious from this timeline, CBMs alone have not succeeded in ending all conflicts and territorial clashes, or in assuring that there is no outbreak of violence. Instead, there have been violent outbreaks and a breakdown of confidence-building measures in 1965, 1971, 1994, 1999, 2000, 2001, and most recently in 2013. Historians describe India and Pakistan as having fought three major wars and one undeclared war. In each case, it has taken the actions of the international community to bring both players back to the negotiating table.

For this reason, analysts disagree about the long-term effects of confidence-building measures. Hilali describes the goal of confidence-building measures as "the gradual creation of an atmosphere of mutual trust, transparency and predictability in slow and incremental steps."[23] Indeed, confidence-building measures in the Indo-Pakistan area include reciprocal visits and exchanges between military experts within a field of expertise, cooperation on related issues (such as oil spills or fishing rights in the maritime environment), and shared emergency-response procedures (to respond to events like humanitarian disasters). Nations may also cooperate in carrying out activities like mapping and surveying the territory or responding to the activities of third parties like terrorists or pirates. Others, however, suggest that territorial CBMs are by nature fragile, and that they represent a "least worst option" for diffusing conflict in a region, but that they are not likely to alter the relationship between adversaries over the long term.[24] In considering events

in India and Pakistan, P. K. Ghosh suggests that no real progress has occurred in terms of increasing trust between the two nations.[25] Rather, the fact that such extremely detailed agreements between the two nations are still needed (i.e., a prohibition on "buzzing" each other's ships with aircraft in the maritime environment) is evidence not of how far the two nations have come, but rather of the tensions that still exist and must be carefully managed.

In addition, nations agreeing to subject themselves to territorial confidence-building measures risk giving up some measure of national sovereignty, since agreements tend to be multinational and to be carried out under the auspices of international organizations like the United Nations (UN). Definitions and ethical standards for determining whether or not a territorial incursion has occurred are thus drawn from customary international law, including the Law on Armed Conflict, rather than from national understandings.

In evaluating the utility of territorially based confidence-building measures, it is useful to consider the so-called "Atlantique Incident," in which a Pakistani naval aircraft was downed by an Indian MIG-22 on August 10, 1999. All 16 people on board were killed. India's government alleged that the Pakistani plane had violated Indian airspace and that the Pakistani military failed to warn India of its intent to fly near the border, which is in violation of the 1991 agreement, and alleged that it had been a spying mission. Pakistan, in response, claimed that the aircraft had made an honest mistake and strayed accidentally into India's territory. The Atlantique Incident is widely considered a failure of confidence-building measures. Procedures like a hotline were in place to prevent misunderstandings of this type, but they were not utilized. The incident

occurred quickly, and it was unclear to what degree the two Indian MIG pilots had acted on their own initiative in shooting down the plane or whether they had been instructed to do so by authorities within the military. This incident calls into question how effective procedures for addressing conflicts ultimately may be when tensions are high and decisions are being made quickly. Hilali argues that this incident occurred, at least in part, because neither side was truly committed to utilizing procedures for addressing and minimizing conflicts, and because neither side actually trusted the other, despite the existence of decades of attempts at cooperation.[26]

Prospects for Success or Failure of Territorially Based Confidence-Building Measures in Cyberspace.

Many key CBM provisions for cyberspace are closely patterned upon existing territorial confidence-building measures. Like other types of territorial confidence-building measures, confidence-building measures in cyber territory are being established and carried out by international organizations. Currently, the ITU is involved in building confidence and security in the use of information and communications technologies.[27] At the same time, the Stanford University Center for International Security and Cooperation has proposed the creation of an international agency with regulatory authority that would be responsible for creating and administering an international treaty to deal with cybersecurity.[28]

In establishing a secure, stable, and predictable environment in cyberspace, leaders have taken steps to provide advance notice and share information

regarding activities like military exercises in cyberspace. Richard Clarke and Robert Knake have called for the creation of a treaty modeled upon the Strategic Arms Limitation Talks (SALT), established to regulate the creation, stockpiling, and deployment of nuclear arms between the United States and the Soviet Union. Clarke and Kane's "cyber war limitation treaty" would include the creation of a risk reduction center, which would act to diffuse crisis situations, coordinate with the UN, exchange information, and work with nations to establish international law concepts.[29]

In addition, the United States and Russia have established several procedures for sharing information in crisis situations to prevent escalation. This includes the establishment of a White House-Kremlin hotline as part of a bilateral agreement on information and communications technology security. This same agreement also calls for creating a U.S.-Russian Cyber Working Group, as well as establishing links between Computer Emergency Response Teams (CERTs) in both countries.[30]

In considering the evolution of confidence-building activities between India and Pakistan in reference to their border regions, it is clear that issues between India and Pakistan increasingly have concerned the actions of nonstate actors. In several cases, cross-border violent activities have occurred, creating situations where it was difficult for participants and the international community to assign responsibility definitively to a particular state. In particular, India has alleged that terrorists and insurgents acting in India in actuality have been sponsored by Pakistan. The activities of nonstate actors and the attribution problem thus constrain the effectiveness of confidence-building

measures of a territorial nature, whether in material territory or in cyber territory.

In addition, the Atlantique Incident shows how military doctrines regarding response to an incursion clash with military-diplomatic agreements regarding conflict prevention. Here, the philosophy behind confidence-building measures was not translated into tactical guidance given to warfighters on the ground or in the air. Similarly, doctrines like active defense in cyberspace are at odds with confidence-building measures in cyberspace as they are currently specified. As David Rickards of the U.S. Naval War College points out, there exist significant doctrinal gaps in the guidance that commanders and warfighters receive regarding how they should respond during situations of cyber attack when they may have only limited communications infrastructure.[31]

Dorothy Denning and Bradley Strawser describe two types of active cyber defense that might be problematic in this regard. First, they describe blocking as "akin to a missile defense system that shoots down incoming missiles or jams their radars and seekers." Secondly, they describe pre-emption as "like launching an offensive strike against the air or ground platform launching the missiles."[32] Both tactics require an immediate response and may require acting in a situation of incomplete information. Because of the rapid speed at which cyber warfare occurs, active defense may also include provisions to pre-delegate authority to carry out defensive actions to cyber warfighters, or even to create conditions in which machines might respond autonomously to perceived attacks without waiting for or even seeking permission. In such a situation, it is difficult to see how confidence-building measures such as the creation of a crisis hotline would be effective in preventing escalation or preventing

misunderstandings.[33] (As Rickards points out, there have been few opportunities to thoroughly test the effectiveness—and the problems—of these doctrines under real world combat conditions, since there has not yet been a full-scale cyber war.)[34]

Denning and Strawser also describe "noncooperative defenses," including so-called "hack backs," which may include a defender responding with an initiative that attempts to get the attacker to install spyware on his system.[35] Here, the hack-backer is often a civilian working in the computer security industry, and it is unclear what legal status such activities may have under a confidence-building measures agreement. Further, such countermeasures might be categorized as spying or covert activities that would be at odds with the values of transparency and trust, which are at the heart of confidence-building measures.

Thus, in order for confidence-building measures in cyberspace to be truly effective in addressing the security dilemma and decreasing the risk of escalation, CBMs aimed at increasing transparency (like advance notification regimes) would also need to be supplemented by more far-reaching CBMs that directly constrain military actors by requiring them to work with other states' parties to discuss and agree upon military doctrines. (Such CBMs have, in fact, been undertaken in the field of nuclear conflict.[36]) In addition, it would be advisable for partners to a CBM agreement to consent to a list of facilities that would not be targeted during a cyber war, to include so-called supervisory control and data acquisition systems, those which run industrial processes, from power plants to electrical grids.

It would also be useful for all players to come together to discuss, and possibly even to agree upon, particular doctrines that would be utilized by all sides in

a conflict, as well as doctrines that would be regarded as unethical, unlawful, or immoral by all sides. Here again, there is precedent for such a discussion since these types of conversations took place among parties to arms control agreements in the field of nuclear war during the 1970s. The aim here would be to develop a shared vocabulary and set of understandings regarding doctrinal developments in the field of cyber warfare so that all parties had the same understanding of concepts such as cyber deterrence and preemptive cyber warfare.[37]

As this short case study illustrates, there are several lessons that those interested in creating confidence-building measures in cyberspace might thus draw from the historical example of territorially based confidence-building measures between India and Pakistan. Figure 3 spells out a few of these lessons.

Lessons Derived from Indo-Pakistan Confidence-Building Measures

As the example of the over 50-year process of establishing confidence-building measures between Pakistan and India shows:

1. The creation of confidence-building measures to mitigate territorial disputes and tensions is a very long process characterized by periods of relative success alternating with situations that clearly show the failures and limits of these agreements.

2. Norms do not always develop over time nor is trust always created.

3. Nonstate actors and the problem of attribution complicate the situation. Military doctrine and tactics may be at odds with the philosophy of confidence building.

4. Territorial confidence-building measures do not occur in isolation: India and Pakistan were forced to cooperate on key issues such as water rights

Figure 3. Lessons Learned from Indo-Pakistan CBMs.

and shared resources. This helped to establish the likelihood that they would also address their military conflicts. Similarly, policies regarding the regulation of territorial conflicts and incursions in cyberspace will be developed and implemented in a broader diplomatic environment where other issues between states may complicate the carrying out of cyberspace CBM's. Here we may consider the fact that Russia's territorial incursions into "real space" in the Crimea are occurring simultaneously with suspected cyber incursions into the same territory.*

5. It is easier to establish territorial confidence-building measures when both nations are stable and subject to regularized elections and turnover in office. Domestic political instability in both India and Pakistan made it more difficult to establish long-term territorial CBM's.

6. The media plays a role in sensationalizing claims that do occur. During the Atlantique incident, tensions flared as leaders in both nations utilized the media to put forth their version of events. Again, events do not occur only at the diplomatic or military level or in isolation from the rest of society.

* For more on point 4, see Jason Rivera: "Has Russia Begun Offensive Cyberspace Operations in Crimea?" *Georgetown Security Studies Review Blog*, March 2, 2014, available from *georgetownsecuritystudiesreview.org/2014/03/02/has-russia-begun-offensive-cyberspace-operations-in-crimea*, accessed on May 12, 2014.

Figure 3. Lessons Learned from Indo-Pakistan CBMs. (cont.)

CASE STUDY 2: BIOWEAPONS

Prospects for Applying Weapons-Based Confidence-Building Measures to Cyberspace.

Although the predominant model that policymakers have used to think about confidence-building measures in relation to cyber is that of territorial CBMs, there have also been limited attempts to utilize a weapons-based CBM model. In particular, Marietje Schaake, a Dutch member of the European Parliament, has been

active in an effort called "Stop the Digital Arms Race." She has called upon European Union members to give the European Commission a mandate to draft legislation and pursue initiatives leading to a weapons ban on the use of "digital arms."[38] In addition, within the European community, some initiatives aimed at combatting cyber crime actually appear to resemble cyber weapons bans or nonproliferation initiatives for cyber weapons. In particular, the 2001 Council of European Convention on Cybercrime attempted to criminalize the "production, sale, procurement, and distribution of devices, including computer programs designed or adapted primary for the purposes of committing offenses such as illegal access, illegal interception and data interference."[39] This same agreement also established regular consultation groups that would bring together parties to share information on significant legal, policy, and technological developments related to cyber crime.

In addition, in the past year, a number of Western nations have taken steps to address problems of weapons transfers of digital arms and the problem of cyber weapons proliferation. In May 2014, the Wassenaar Arrangement, an export license agreement signed by 41 nations and originally established to track the production of components used in the manufacture and production of biological and chemical weapons, was amended to include new provisions requiring states' parties to track and regulate what types of software code was being exported through sales to clients abroad. This development was due in large part to recent revelations showing that the German program FinFisher, used by law enforcement to "snoop" on the transactions and files of those suspected of engagement in criminal activity, had been exported to many

authoritarian regimes that were using the program to spy on their own citizens. The official response to the FinFisher revelations from both the United States and the Organisation for Economic Co-operation and Development was to condemn the company for having violated guidelines on the export of this product.[40] However, academic computer scientists were equally shocked, with many expressing a desire to work together with law enforcement and other agencies to ensure that their work was not used against citizens in this way. The Wassenaar arrangement includes controls on zero days and other types of intrusion and surveillance software.

However, critics have pointed to shortcomings with this development. Jennifer Granick argues that the challenge will be in defining which types of vulnerabilities should be placed on this list, voicing the concern that defining the class of restricted tools too tightly would hamper the ability of academics and private sector security consultants to conduct research in the area of computer security. There is also a concern that in making one class of cyber weapons components more difficult to procure, those wishing to manufacture such weapons will simply move on to the creation of different weapons.[41] Furthermore, this international agreement, even if effective, will do nothing to stem the problem of nonstate actors who might seek to acquire or utilize these components.

Finally, as Granick points out, the agreement is not legally binding (that is, it does not have the same legal status as a treaty), and it will be up to each state individually to undertake the creation of domestic legal and administrative procedures in support of the agreement. The ability of states to do so may depend on domestic political and economic factors, as well as the overall level of development of each state.

The FinFisher incident and the subsequent adoption of the Wassenaar arrangement, however, is a powerful illustration of the role which technical specialists and civilians play in the creation of CBMs for cyber weapons. The cyber weapons community consists of government officials, including military members and civilians, including those with commercial interests in the sector, as well as academic scientists who may be involved in developing innovative new weapons technologies. In carrying out confidence-building measures, government officials need to work with commercial and academic actors, being careful to respect the interests of all players and seeking to influence and guide developments without being seen as seeking to control that process unduly. As President Barack Obama wrote in his 60-day review of cybersecurity operations in February 2009, "the private sector designs, builds, owns and operates most of the digital infrastructure."[42]

In implementing the Wassenaar Arrangement, the United States will task the Department of Commerce with issuing export-licenses for software. Code is thus regarded not as a military munition subject to military regulation, but rather as a commercial good subject to commercial regulation. Similarly, unauthorized trafficking in this commercial good is regarded as a criminal matter, rather than a security matter. In this situation, the locus of authority has changed, with the Department of Defense (DoD) taking a backseat to other federal agencies involved in regulating cyber weapons. The lessened role for DoD is not surprising here, since as Deibert suggests, a new model of CBMs that involves practitioners and civil society in describing conditions of use for cyber weapons, and developing norms for their use represents a break with traditional realist cyber strategies.[43]

The Wassenaar example is instructive because it illustrates the ways in which norms governing the proper role and use of both offensive and defensive cyber weapons can, in point of fact, emerge organically through the contacts and cooperation that will take place between practitioners. Thus, while territorially based CBMs attempt to create norms regarding proper conduct in cyberspace, which are then imposed upon participants in a top-down pattern, the example of the Wassenaar arrangement shows how policymakers can perhaps create the conditions for practitioners to have a stake in developing these norms and taking responsibility for the sorts of weapons that are developed and deployed. As the adoption of the Wassenaar arrangement shows, technical specialists who produce cyber weapons have their own strong normative ethos regarding the situations in which it would be proper and improper to deploy such weapons, and they are willing to invest in procedures to secure these cyber weapons.[44] In this way, they resemble the medical personnel who decided in the early-20th century that contributing to the production and stockpiling of biological or chemical weapons was against their ethos as a medical community, which should be committed to healing patients, not harming civilians.[45]

Because bioweapons and cyber share so much common ground in terms of challenges to detection, verification, and monitoring, it makes sense to consider both whether the same CBMs can be used in both instances and how effective those CBMs are. As Figure 4 shows, there are many similarities between the two weapons classes in terms of their possible uses, as well as issues for monitoring and verification. However, there are less similarities when it comes to the existence of an international consensus or set of norms regarding their possible use.

		Biological Weapons	Cyber Weapons
Strategic Use	Confer Advantage to Attacker	X	X
	Can be used as force multiplier with conventional attacks	x	x
	Poor deterrent	x	x
	Asymmetric weapon	x	x
	Produced and deployed quickly (no lead time to produce	x	x
Issues for Monitoring	Difficult to detect production facilities	x	x
	Minimal non-detectable byproducts produced in manufacture	x	x
	Cheap to manufacture	x	x
	No lead time for production	x	x
	Ability to carry out zero day exploit	x	x
	Attribution problem (no signature)	x	x
International Consensus	Normative consensus that these weapons are immoral	X	No
	Consensus against using on civilians	X	No

Figure 4. Comparing Biological and Cyber Weapons.

As this figure illustrates, biological and chemical weapons share common ground with cyber weapons in terms of their utility, cost, and likelihood of deployment. As Gregory Koblenz notes, in a biological weapons conflict, the individual who attacks first has the advantage, as these weapons have greatest utility when they are used in an offensive capacity. In addition, as with cyber weapons, these weapons may have great utility when used as a force multiplier for conventional weapons deterrent strategies.[46] Biological weapons, like cyber weapons, also confer the advantage that, unlike kinetic attacks, they do not destroy their target. Finally, both types of weapons can be used to disrupt a society in order to then carry out activity using conventional weapons. In the cyber realm, General Keith Alexander, Director of the National Security Agency, has referred to cyber weapons as useful for carrying out Phase Zero operations such as wiping out an opponent's communications infrastructure prior to launching a conventional attack.[47]

Like cyber weapons, biological weapons do not work well in a deterrent capacity. As Koblenz points out, the uncertainties associated with deployment of biological weapons as well as the fact that they can be manufactured largely in secret means that they do not work well to threaten one's opponents.[48] In addition, those who do manufacture these weapons are not likely to broadcast their particular characteristics since to do so risks losing one's advantage in research and development. Thus, they are a powerful secret weapon but not a powerful deterrent.

Like biological and chemical weapons, cyber weapons can be produced relatively cheaply in large quantities, often without a large risk of detection. Biological weapons can be manufactured through

the assembly of parts that are easy to find and readily available and the risk of detection is low (as with cyber weapons). As Theodore Karasik notes, the components used to manufacture biological and chemical weapons can be found at airports, farms and garden supply warehouses, college laboratories, barge terminals, electronics plant manufacturers and storage areas, glass and mirror plants, pipelines and propane storage tanks.[49]

Because it is possible to manufacture both biological/chemical weapons and cyber weapons without investing in infrastructure like a factory or processing plant, there is also not a lot of lead time from when one makes a decision to engage in their manufacture to when one's production facility is operational. Weapons of this type are thus cheap, easily deployable, and offer a great deal of flexibility to their developers.

Biological and cyber weapons also both present a "dual use dilemma." In the case of biological weapons, Filippa Lentzos describes the fact that the 1975 Convention of Biological Weapons and Toxins explicitly outlaws measures "that enhance the virulence, toxicity or antibiotic resistance of pathogens (including through the use of genetic engineering), synthetic production of toxins and examining biological aerosols." However, he points out, in 2000, DoD researchers engaged in research into weaponized anthrax for the purposes of developing better vaccines for soldiers. As he notes, the main factor separating out the use of biological weapons for research purposes from the use of biological weapons for warfare purposes is simply that of intent.[50] In actuality, the two types of activities look very much the same to an observer. Similarly, researchers attempting to perfect defenses against cyber weapons often engage in activities, including hacking,

which look very similar to attempts to carry out cyber warfare. In addition, defending against both biological and cyber weapons can be extremely costly. A state can easily expend vast resources in vaccinating civilians and military specialists against suspected pathogens, and a government agency or commercial facility can easily spend millions or even billions of dollars to create and update software and hardware procedures to defend against suspected computer viruses.

Like cyber weapons, biological and chemical weapons also come with an attribution problem. They seldom possess any sort of unique signature that would make it possible for them to be traced back to a particular manufacturing plant, individual or group.[51] Like cyber weapons, there are no incriminating waste products produced in their manufacture as there is in the manufacture of nuclear weapons, for example.[52]

Because it is often so difficult to prove that a state (or nonstate actor) has actually engaged in the manufacture or production of these types of weapons, it is possible to argue that the sorts of regimes utilized to monitor and verify claims about their production are not particularly useful. Indeed, in all of the recent legal cases that have been undertaken in which it was suspected that a state had indeed produced and even deployed these weapons, the bulk of the evidence did not come from international monitoring agencies or even law enforcement, but rather from intelligence reports gathered covertly. That is, monitoring regimes are what one utilizes "in theory," but in point of fact, intelligence is far more useful for gathering information about the deployment and use of these types of weapons.[53]

In addition, biological and chemical weapons offer the advantage that they (like cyber weapons) can

be used to conduct zero-day exploits. In both situations, it is possible for a weapon to deploy without the target even knowing that it is under attack. Observers may not perceive that an attack is ongoing, and it may only be in retrospect that a target even becomes aware that an attack has occurred. Here we can draw a parallel between the epidemic of food poisonings that occurred in the western United States that were later determined to be a type of bacterial warfare attack carried out by the religious cult, the Rajneeshis, and the Stuxnet attacks on uranium processing and production facilities carried out in Iran. In both cases, targets were not aware that the attacks were occurring, and, even in retrospect, there were questions about attribution and the timing of attacks.

Finally, both biological warfare and cyber warfare, like nuclear war, present the possibility of doing such long-term worldwide damage that the results might be world-ending or apocalyptic.[54] Cyber warfare might include elements like an electromagnetic pulse, which could destroy all modern communications, while deployment of biological agents could damage the gene pool for generations to come. In this way, one can argue that cyber warfare spirals also present a risk of mutually assured destruction, similar to the risk that many argue was the best reason why nuclear arms risk reduction talks were successful in preventing nuclear war. In this way, both biological/chemical and cyber weapons confer an advantage to the attacker, and they appear to elude simple solutions such as prosecuting those who engage in them. For that reason, the emphasis needs to be on preventing the manufacture of these weapons, rather than merely responding to their deployment once it occurs.

Figure 5 provides a timeline of the steps taken to implement confidence-building measures for biological weapons. As the figure shows, the history and timeline for establishing weapons-based CBMs differs somewhat from the history and the timeline for establishing territory-based CBMs described earlier. This is largely because the term "confidence-building measures" itself means something different within the context of a weapons ban. While territory-based confidence-building measures aim to create transparency and information sharing procedures in order to mitigate conflict and create a stable environment, the weapons-based confidence-building measures described here are aimed instead at enforcing a ban on or controlling the production, stockpiling, and use of these weapons through creating measures for sharing information and allowing verification so that all parties to the treaty adhere to the regime and so that those who do not comply with the regime are punished.

Timeline of Activities Associated with Confidence-Building Measures for Biological Weapons

1925: Passage of Geneva Protocol prohibiting use of biological and chemical weapons (but not their manufacture or stockpiling).

1942: United States establishes a biological weapons program at Ft. Detrick, MD.

1969: United Kingdom and Warsaw Pact introduce proposals to UN for a ban on biological and chemical weapons.

1970: United States renounces its biological warfare program.

Figure 5. Confidence-Building Measures for Biological Weapons.

1972: UN creates Biological and Toxin Weapons Convention.

1975: Treaty enters into force with 46 signatories.

1979: Anthrax outbreak in Sverdlovsk, Russia widely believed to have occurred due to experimentation with biological weapons. Soviets denied engaging in biological weapons research until 1992 when they officially acknowledged their programs.

1980's: Iraqi President Saddam Hussein launches an aggressive biological weapons program.

1984: France and China join convention.

1984: Rajneeshis Cult in Oregon is accused of engaging in biological warfare through poisoning salad bars in the United States.

1991: In the aftermath of Gulf War, UN Special Commission (UNSCOM) conducts inspections of facilities in Iraq suspected of carrying out production of biological and chemical weapons.

1992: In order to become a signatory to the Biological Weapons Convention, Russia shared with the United States and United Kingdom its draft declaration on past and present biological weapons activities, including admitting having maintained an offensive biological warfare program from 1946 to March 1992 – though it claimed it was only in the prototype stage.

1994: Creation of Ad Hoc Group of States' Parties in an attempt to negotiate more legally binding verification regime for biological weapons convention.

1999: Beginning of development of codes of ethical conduct for scientists working in the field of biological weapons with statement by British Medical Association.

Figure 5. Confidence-Building Measures for Biological Weapons. (cont.)

2001: U.S. Capitol is shut down due to anthrax mailed to Congress people, journalists and others in the United States.

UN fails to reach agreement on a verification protocol for Biological and Toxic Weapons Convention (BTWC).

United States rejects verification protocol and proposes new changes to strengthen the BTWC, including the creation of a universal code of ethical conduct for bioscientists.

2013: U.S. Capitol receives envelopes containing ricin, a poison, in the mail.

2014: Today, there are 163 signatories to this treaty. However, many states do not submit the required annual reports or submit reports that are insufficient.

Figure 5. Confidence-Building Measures for Biological Weapons. (cont.)

The Development of Weapons-Based Confidence-Building Measures.

In examining the growth of confidence-building measures aimed at banning biological weapons worldwide, it is necessary to acknowledge the importance of a precipitating event—namely the deployment of chemical and biological weapons during World War I—which led to the establishment of a normative consensus against the use of both chemical and biological weapons. In regards to biological weapons, the German government was accused of attempting to poison and infect British livestock, as well as of stockpiling plague with the intent of poisoning Russian citizens and weakening their resistance.

In the aftermath of World War I, both biological and chemical weapons were regarded as problematic since they failed to distinguish between military and civilian personnel and were indeed most efficient when deployed against major population centers, often through the use of airplanes.[55] In the aftermath of World War I, there was thus a strong public outcry against the continued use of these weapons, and strong public support for measures that would ban their use in future wars. This led to the adoption of the 1925 Geneva Protocol. However, even before 1925, there existed strong taboos against the use of chemical and biological weapons. Some historians point all the way back to writing in the Greek city-states, which suggested that the use of poison was duplicitous and cowardly and, even then, seen to violate the laws of war. Margaret Hallissy notes that "the poisoner" was seen as using his "superior secret knowledge" to compensate for his physical inferiority. In that way, poison was seen as a less manly form of warfare.[56]

This consensus resulted in language forbidding the use of biological and chemical weapons being inserted in the 1925 Geneva Protocol and is seen as the reason why biological and chemical weapons were never deployed during World War II. However, the Geneva Protocol was not yet a robust tool for banning the use of chemical weapons, since it banned only the first use of biological weapons, without addressing the problem of the acquisition of weapons. The document also allowed for "reprisal in kind" if the state was attacked by another state using chemical weapons. At the time of adoption, this concept was hotly debated. In the words of Guillemin: "Ostensibly, it allowed limited or symmetrical use of a prohibited weapon, if it were undertaken to persuade an adversary using

the weapon to stop. Whether reprisals in kind against civilian populations fit this exception was a matter of contention."[57] It thus represented a consensus regarding the development and stockpiling of biological and chemical weapons but not regarding reprisal, retaliation, or justified first use.

However, despite the adoption of the Geneva Protocol, many nations, including the United States, began engaging in biological weapons research during World War II. In the late-1960s, however, nations again began agitating for the creation of a ban on biological weapons. The strong worldwide reaction against the use of napalm in the Vietnam War is implicated in the passage of the 1972 Biological Weapons Convention.[58] In this case, the public outcry was particularly strong regarding the deployment of chemical weapons against civilians.

Thus, the passage of both the 1925 Geneva Protocol and the 1972 Biological Weapons Convention can be seen as the acknowledgement and codification of a norm that was already existing and widely accepted, rather than being attempts at establishing a consensus and building a norm. (Indeed, Guillemin notes that even Hitler himself spoke out against the use of chemical weapons.[59]) In each situation, the norm grew organically from the bottom-up, rather than being imposed in a top-down fashion from an outside organization. The biological weapons example thus shows that confidence-building measures can either recognize or codify a preexisting norm or work to establish a norm. In the case of norms involving weapons, it appears that confidence-building measures often rest on a preexisting norm that the weapon itself—or its modes of deployment—is both morally and ethically problematic.

However, one can also argue that those nations that agreed to ban the production, stockpiling, and deployment of biological weapons did so not out of any ethical or normative commitments, but rather due to realpolitik. That is, states made a rational decision to support a biological weapons ban due to the opportunity costs associated with the creation of these weapons; the uncertainties inherent in the development of new technologies; and ultimately the possibility that such weapons, once used, could easily spiral out of control, inflicting potentially permanent damage to the environment and population. Here, Mark Wheelis, Lajos Rozsa, and Malcolm Dando argue that the tactical and strategic advantages of using biological and chemical weapons are simply insufficient for the U.S. military leadership to be fully committed to either the development or deployment of these weapons. Thus, they suggest that the United States has always done just enough to be competitive in this field and not to lose their advantage.[60]

Finally, in a situation where a strong international preexisting norm against the deployment of a weapon thus exists, we may expect that when a weapon is deployed (or where there is a strong suspicion that a weapon has been deployed), the force of international public opinion will be strongly against the nation or group suspected of deploying the weapon, regardless of any justification which the actor might furnish. In the words of Guillemin:

> Unless a state can afford to retreat from world opinion, the use of chemical weapons identifies a user state with a kind of ruthless barbarism, as it did when Iraq used them against defenseless Iranian troops, including children, in the 1980s Iran-Iraq War.[61]

Similarly, Richard Price refers to chemical weapons as "an object of special opprobrium."[62] In this way, the international taboo against the use of biological weapons serves to dilute their military utility, rendering them a less desirable and less effective form of warfare.[63]

Wheelis, Rozsa, and Dando thus argue that the main reason that the United States is not a powerhouse in the deployment and manufacture of biological or chemical weapons is simply because they do not want to be, rather than because of either a strong system of monitoring and verification restrictions that precludes doing so, or even out of a deep-seated ethical and moral sense that it is improper to do so. They essentially state that the chemical and biological warfare advocates never had the kind of leverage they needed to develop an adequate biological weapons program. The program was never a serious priority—advocates of biological weapons tended to see their program in isolation, not as a component within the entire weapons program. In addition, chemical and biological weapons were never fully integrated into either military doctrine or forces. Military men generally did not feel comfortable with these weapons.[64]

Thus, some analysts have suggested that it is not confidence-building measures that have reigned in the use of biological and chemical weapons in the 20th and 21st centuries, but rather the strong ethical and moral taboos that historically have accompanied the deployment of these weapons.[65] In addition, Guillemin suggests that nations like the United States, France, and Germany were willing to trade their interests in manufacturing and deploying biological and chemical weapons in the 1970s because they possessed the security of a nuclear umbrella. Thus, using biological

and chemical was always less desirable when other options were available.[66] Reducing the supply of such weapons is thus less problematic when there is already less demand for these weapons, for moral and ethical reasons.

The question is thus whether we will ever see a similar international consensus regarding the need for a ban on the development, production, and deployment of cyber weapons, and whether states would ever decide that it is not in their interest to develop cyber weapons. If there does not exist a similar consensus regarding the immorality and undesirability of using cyber weapons, can one be built? Here we can point to, in more recent times, the passage of protocols that would forbid the deployment of nuclear weapons as well as current attempts to outlaw drones and other forms of autonomous killing. In each instance, the introduction of new technologies led to a public conversation about the ethics and morality of a particular new warfighting technology, from the introduction of automatic weapons to the introduction of landmines to the introduction of nanotechnology. That is, in the immediate aftermath of the introduction of new technology, there exists a window for the establishment of new norms regarding the deployment of that technology, as well as for a public conversation that might include scientists, weapons manufacturers, and those who will eventually be responsible for its use. It is thus not warfare itself with the new weapon that leads to this conversation, but rather the introduction of new technologies rendering the weapon possible that does so.

Thus, one may query whether it is useful to compare confidence-building measures against the use of biological and chemical weapons with confidence-building measures against the use of cyber warfare since, at least at present, there does not appear to be a strong set of moral arguments against the deployment of cyber weapons. The supply of such weapons is still great, as is the demand for these weapons. Indeed, those who create cyber weapons have made the argument that cyber weapons are actually more moral than conventional weapons or weapons of mass destruction, since they often only disrupt rather than destroy, and it is not clear whether any specific deaths can be attributed to cyber warfare alone in the present era. In addition, there is no consensus among states regarding the appropriate role or stance for government to take in regulating the Internet at all, whether as a domestic technology or an international vehicle. States differ in their stances regarding issues like Internet censorship, Internet surveillance, and pricing schemes for Internet usage, including whether the state should subsidize the costs of Internet usage. If states do not share a consensus regarding their stance toward the Internet as a utility, can we also assume that this makes it unlikely that states will share a consensus regarding the development and possible deployment of cyber weapons?

In addition, as Sofaer, Clark, and Diffie point out, states may be less willing to cooperate and form regimes in order to eliminate a type of weaponry when the technology that created the weaponry is still quite new.[67] Scientists and policymakers may feel that they have not yet had sufficient time to explore the full capabilities of cyber weapons, both in an offensive and defensive capacity, and thus agreeing to limit their use at this time is premature. Agreeing to limit their deploy-

ment represents a risk since all parties are not entirely sure at this stage what specific future utility they may be agreeing to forego.[68] In a situation where much of the progress in this field will be made by commercial actors, any moves to limit the development or deployment of these new technologies might also be seen as a financial risk. Here we might consider, for example, attempts by the European community to limit the development of genetically engineered foods. While policymakers may have felt that the risk posed by genetically modified organisms was sufficient to implement legislative controls on this technology, European firms have complained that they are being placed at a competitive disadvantage by being prevented from engaging in research and development in this field since other firms in other nations will continue to develop these technologies. They have also opposed the fact that government entities are attempting to limit current profits for the sake of limiting future risks.

Furthermore, neither the United States nor its adversaries (like China or Russia) seem to believe that cyber warfare is a less desirable or second-best plan of either offense or defense. States may be invested in retaining arsenals of cyber weapons and may not see any sort of ethical issues with doing so. Indeed, in his work, Kirk Bansak argues that establishing regimes that would disallow the use of one type of weapon may actually backfire, creating unintended and unanticipated new scenarios. He argues that those who seek, for example, to outlaw all use of biological weapons may actually be pushing both state and nonstate actors who might have previously sought to use biological weapons to instead up the ante, choosing to deploy yet a more deadly class of weapons, now that the use of biological weapons is off the table.[69] Thus,

an attempt to ban the use of biological weapons might cause an adversary to go nuclear, and an attempt to ban cyber weapons might simply increase the likelihood of conventional warfare.

However, it is possible for a state to push for a ban on the development of new weapons not because of any implicitly ethical agenda, but rather for pragmatic reasons. Thus, it has been suggested that the push by the Shanghai Cooperation Organization states in 2011 for the formation of a set of norms governing cyber conflict arose not out of a genuine willingness to reduce conflict in this area, but rather was part of a realpolitik strategy. Worried that their nations could not compete in a cyber arms race, the parties instead chose to agitate in favor of ending such an arms race. In doing so, they lessened their risk of defeat in an arms race as well as their domestic costs of conducting additional research and development.

While states may thus be pessimistic about either the likelihood of a long-term ban on the development of cyber weapons or the development of an ethic against their use, it is still useful to think about the ways in which verification and monitoring regimes might be put into place in the area of cyber weaponry, again based on the example of biological and to a lesser extent chemical weapons.

Provisions for Verification and Monitoring.

Like the territorial confidence-building measures described earlier, the CBMs for biological weapons are quite extensive. In the Seventh Review Conference on the Biological Weapons Convention, which took place in 2011, participants agreed to seven separate sets of confidence-building measures.

1. Exchange of data on research centers and laboratories.

2. Exchange of information on national biological defense research and development programs.

3. Exchange of information on outbreaks of infectious diseases and similar occurrences.

4. Encouragement of publication of results and promotion of use of knowledge.

5. Declaration of legislation, regulations, and other measures.

6. Declaration of past activities in offensive and/or defensive biological research and development programs.

7. Declaration of vaccine production facilities.[70]

In this way, it becomes clear that the implementation of CBMs in this area cannot be carried out by one agency alone but rather that it requires an interagency effort on the federal, state and local levels. Regulating biological and chemical weapons thus becomes a matter of international policy, as well as domestic policy.

Figure 6 provides a graphic representation of the various social and political sectors involved in carrying out CBMs having to do with biological warfare. In particular, Article IV of the Biological Weapons Treaty requires states to adopt national measures that allow them to comply with treaty provisions, including Article 1. However, the implementation of national or domestic measures to uphold the provisions of the Biological Weapons Treaty has occurred in an inconsistent manner among signatory nations.

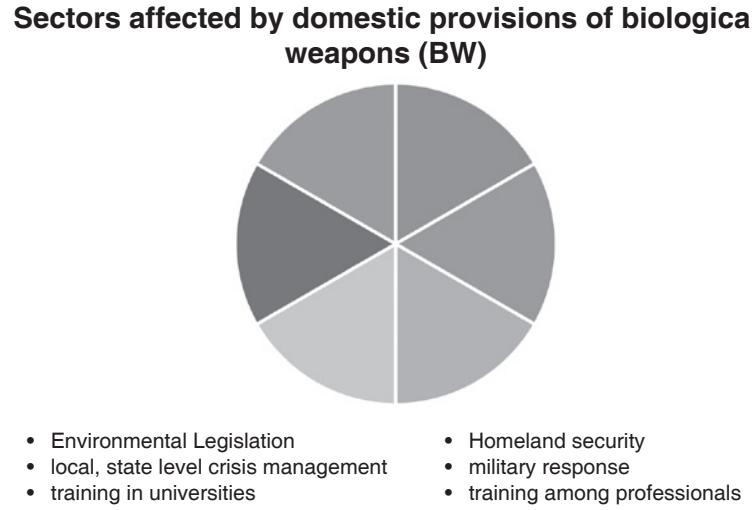


Figure 6. Domestic Effects of Biological and Toxic Weapons Convention.

The convention specifically allows states to choose how to implement these national measures in accordance with their own forms of governments and constitutions. As such, implementation measures may include legislation, regulations, government decrees, or administrative orders. In addition, the treaty requires that states establish criminal penalties for those found to be violating core provisions of Article 1 through, for example, developing, producing, stockpiling, or acquiring biological weapons.[71] Again, these penal sanctions may end up looking very different depending on the type of legal and governmental systems in place within a particular nation. Here, the danger is that penalties might be applied and enforced inconsistently.

In considering CBMs for cyber weapons acquisition and proliferation, we must consider how states

can be encouraged to undertake domestic measures to outlaw or regulate cyber weapons and how they can encourage private sector actors to buy into these processes. This would involve writing legislation that would more tightly regulate the companies currently providing computer security, perhaps mandating them to provide and share information. (Many industries currently do so voluntarily but the provision is inconsistent). In addition, UN Security Council Resolution 1540 requires all signatory states to the Biological Weapons Convention to carry out domestic measures (including surveillance) in order to prevent the development and acquisition of biological, chemical, and nuclear weapons by terrorists and nonstate actors within their borders. This provision adds to the domestic regulatory burden in this area, as states are required to implement storage and reporting procedures for chemicals and equipment that can be used in the manufacture of biological or chemical weapons. They are also required to implement effective import and export controls and operate stringent border controls to prevent the proliferation of these weapons of mass destruction.[72]

Here the model provided in the areas of biological weapons surveillance provides best practices for establishing surveillance and response procedures in the areas of cyber weapons use and deployment. In particular, biological weapons surveillance programs like Biosense, Biowatch, and BioPhusion show that local, state, and national agencies, as well as the private sector, can work together to monitor and provide guidance in situations where weapons use is suspected.[73] As can be seen with the example of Biowatch, many of the parties that are asked to abide by regulations and contribute to goals regarding stemming the prolifera-

tion or use of biological weapons are not government employees, whether on the federal, state, or local level. Instead, individuals and groups impacted by this legislation may include pharmaceutical companies, university laboratories, and hospitals. This complicates the situation since undue government intervention into the affairs of a private company and the affairs of private individuals can easily be perceived as government overreach and such activities might even be described as unconstitutional. As a result, a regime has evolved in which (at least in the United States) some activities of parties affected by the domestic provisions of the biological weapons regimes are undertaken on a voluntary basis while others are undertaken due to federal regulations that require subject's compliance.

Another valuable lesson which those looking to implement CBMs in regard to cyber warfare can draw from an examination of biological warfare regimes is in the area of socializing new scientists into the values of an academic community. Under the provisions of the Biological and Toxin Weapons Convention, signatory states agree to implement procedures to raise awareness of the prohibition against manufacturing and developing biological weapons.[74] As a result of these provisions, U.S. scientific and research communities have implemented programs to socialize new members of the academic community into the norms and responsibilities, which they will bear as scientists working within this field. Current U.S. standard operating procedures include requiring scientists and others to undertake training on states' criminal laws banning biological weapons production and deployment and requiring scientists to adhere to a code of conduct requiring them to refrain from working on biological weapons.[75] Thus, a scientist might par-

ticipate in a workshop or conference regarding the ethics of scientists working in the field of biological weapons production voluntarily, while he might undertake other training that is mandated by his university as a condition of receiving U.S. Government research funds.

The biological weapons CBMs thus clearly show the role that the specialist community plays in carrying out almost all of the activities agreed upon—including exchanging data about the existence of research centers and labs; exchanging information on research and development programs; exchanging information on outbreaks, as well as in providing for the publication of results; and in declaring past activities. In each instance, the specialized nature of the information to be shared is specific enough that only scientists can make the sorts of judgment calls that would be required, and for this reason, it is crucial that they share an ethical stance regarding their work and that they are committed to and engaged with the security issues which can result from their work.

Here we can consider the ways in which the biological sciences community was involved in a series of decisions that occurred in the early-2000s. A number of advances in genetic engineering were determined to have utility in the manufacture of new and potentially more deadly viruses. In 2001, American scientists accidentally created a new and more deadly variant of mouse pox while doing research on pest control. In 2002, scientists were able to create an artificial version of the polio virus that was found to have utility to those engaged in biological warfare, and in 2002, researchers were able to sequence DNA in order to learn more about how smallpox works in the body. In each instance, results were published publicly in aca-

demic and mainstream science journals. Policymakers criticized the editor's decisions to publish this material, and the controversy led to a statement by a coalition of science and biology editors' groups stating that in the future, they would consider security issues in deciding what information to publish.[76]

The lessons for the cyber community are clear. Practitioners in the fields of cyber defense must develop an ethic regarding the value of their work and its relation to national security. Specialists play a vital role in self-policing, and it is one that cannot be duplicated by outside actors who do not possess the specialized knowledge that is needed to make judgment calls regarding the implications of one's work.

However, decisionmakers should be aware that the sorts of domestic measures that might be undertaken to deal with either a biological or cyber weapons incident within U.S. borders are likely to be perceived by the press and the general public as problematic. Preparing for a biological warfare event like a pandemic would likely involve the implementation of measures such as mandatory vaccinations, the establishment of quarantines, and the establishment of border controls—all of which could be described as examples of government overreach and antidemocratic activities.[77] Similarly, measures that might be implemented in the area of cybersecurity would likely look similar (including cutting off parts of the Internet and requiring particular types of cyber hygiene) and be met with similar resistance, even if they were implemented as part of an international treaty aimed at securing these weapons. In each case, the government action is aimed at containing a threat and preventing its escalation—each response requires multiple actors working together on all levels of government, including civilians.

Addressing Suspected Violations of the Convention and the International Response.

At the same time, the biological weapons ban did not actually forbid all states from developing or even deploying biological weapons. Rather, there were still suspicions that many nations were continuing to engage in research in the field of biological weapons. Thus, it is worth pointing out that many of the specific provisions of the ban in the areas of verification and monitoring are not viewed as robust within the international community. It is likely that similar problems might arise were states to attempt to verify and monitor the implementation of regimes banning or controlling the development of cyber weapons.

Those that argue the attempts to outlaw the creation of biological weapons are doomed to failure and traditionally have pointed to two specific cases: the robust program of biological weapons research and development carried out by the Soviet Union throughout the 1960s and 1970s, and the more recent case of weapons treaty violations carried by the Iraqi government and the UN Special Commission (UNSCOM) verification mission in the 1990s. Each of these cases points out specific limitations of a weapons treaty, and each may hold lessons for those proposing to establish a similar set of verification regimes in the areas of cyber weaponry.

Case One: Biopreparat and the Former Soviet Union.

In the late-1980s, the former Soviet government admitted that it had maintained a large and vibrant biological weapons program since the 1960s. Jack Beard argues that the Soviets "began cheating on the biological weapons regime less than a year after signing it."[78] Koblenz argues that the Soviet biological weapons program can be compared to a covert activity occurring within a democratic society where even a nation's legally elected leaders might not be aware of all of the details of a program. He describes Biopreparat as "a deliberate maze of false front, secret projects and parallel organizations that often conducted both military and peaceful research. The structure was designed to enhance secrecy."[79]

Full details of the project only came to light in the late-1980s, and only because of a decision by the new Russian leadership to provide details about activities that had occurred under the old Soviet regime, and from which they now wished to distance themselves. Thus, the decision to share information with the international community about treaty violations was the result of domestic political factors and was not the result of any treaty or verification and monitoring regime.

The Russian/Soviet example thus shows that international issues seldom occur in isolation. Rather, transparency in the area of biological and chemical weapons was finally achieved between the United States and Russia not due to any official legislation, but to domestic political developments and the developing relationship between the American and Russian leaders. Thus, in considering America's ability to establish bilateral and multilateral regimes to control the

manufacture, proliferation, and possible use of cyber weapons with Russia, clearly the likelihood of success or failure in this arena will depend on such factors as the preexisting state of relations between the two nations in other areas, the amount of trust or suspicion that exists between the two nations in relation to other issues (such as Russia's invasion of the Crimea, differences between the two nations regarding whether or not to condemn the Assad regime, differences of opinion regarding practices of Internet censorship and policies on gay rights in the two nations) and the personal relationships between the two leaders.[80]

Case Two: The United Nations Special Commission.

In 1991, in the aftermath of the Gulf War, the UN established UNSCOM, which was tasked with investigating whether Saddam Hussein's regime had engaged in treaty violations in the area of biological weapons. The commission, which lasted 7 years, has been described as "the most intrusive arms control regime ever devised," since inspectors were able to engage in unlimited aerial monitoring, to visit any site anywhere in Iraq unannounced, to take photographs and to ask questions of personnel. However, despite the legal force and resources given to UNSCOM, Koblenz describes the initiative largely as failure, arguing that it was only when a high-ranking Iraqi official defected in 1995 that inspectors actually received a true picture of Iraq's activities in these areas.[81]

Thus, one can argue that, regardless of how robust a monitoring regime is, ultimately, intelligence activities will always be more effective than open monitoring, and states will always be able to elude detection if they are committed to doing so. Those who point to the failure of UNSCOM as an indictment of the futility

of engaging in arms monitoring are likely to be similarly pessimistic about attempts to establish a monitoring regime for cyber weapons.

In her analysis of the failures of the Biological Weapons Convention, Iris Hunger describes "transparency" as a concept which is too vague to be useful. She faults the writers of the convention who noted that states needed to "keep the international community informed" of developments in key areas, but stopped short of requiring that states report specific numbers, such as how many doses of vaccine they had prepared. It is this vagueness, she argues, that is at the heart of the culture of rumors that exist within the international community in relation to discussions about biological and chemical weapons treaties and supposed violations.[82]

However, a more serious concern (and one that holds resonance for thinking through how these provisions might work in the establishment of a cyberspace treaty) is that the states that have the most serious problems with biological and chemical proliferation within their borders are also the most unstable nations, with weak structures of state authority and poor mechanisms for enforcing any legislation domestically. Nations like Syria and Libya are either embroiled in or emerging from the chaos of civil war, they often fall within the range of states described as failed states, and their legal structures may be nearly nonexistent. In such a situation, while a treaty may mandate that states pass legislation regarding monitoring, punitive regimes, and reporting requirements, it is doubtful that they will have the wherewithal to seriously carry out such obligations either now or in the near future.

Indeed, N. A. J. Taylor, Joseph Camilleri, and Michael Hamel-Green estimate that currently, eight Mid-

dle Eastern countries have a biological and chemical weapon capability, along with a means of delivery. Indeed, they describe the Middle East as the "poster child" for the failure of global and regional non-proliferation efforts.[83] Similarly, Hanis Haziqah, Md Hambali, Megan Hafizal, Megan Ramli, Noorliza Hamdan, and Zalini Yunus point to the absence of an awareness among scientists in Malaysia about the political and ideological significance of their work, or the development of ethical thinking in this area.[84]

Figure 7 lays out some of the lessons that we may thus draw from considering the enactment of provisions for regulating the development, production and use of biological weapons through the Biological Weapons Convention.

1. In the absence of a catalyzing event, the establishment of a normative consensus or "taboo" regarding the creation of cyber weapons is unlikely.

2. As with biological weapons, the creators of CBMs for cyber weapons will find it difficult to predict the types of weapons that might emerge in the future or the issues associated with them. It becomes difficult to craft a convention on future weaponry in light of this constraint.**

3. Prohibitions on the use of cyber weapons should not be considered in isolation. By making access to one type of technology more difficult, an adversary may simply be driven to utilize other means. Just as outlawing biological weapons didn't end conflict, outlawing or regulating the use of cyber weapons may simply change the shape of conflict by making the use of different weapons more likely.***

4. The development of confidence-building measures for preventing the production, dissemination or use of biological weapons represents only one stage of a larger program of defense in depth. The responsibilities for

Figure 7. Lessons from Confidence-Building Measures in Biological Weapons.

preventing outbreaks of deadly disease are dispersed among a variety of actors throughout society – from individuals who are encouraged to engage in public health measures like getting vaccines, to professional organizations that offer training and monitoring, to the roles of states and international organizations. Similarly, cybersecurity regimes include a regard for cyber hygiene on an individual and corporate level, through the activities of professional societies, up to and including the activities of states.

5. Planners would do well to consider in advance the domestic implications of a cyber weapons regime – including the issues that arise in a democratic society when precautionary or reactive measures are taken.

** These constraints are described in Casadevall, pp. 584-587.

*** This is the argument found in Bansak, pp. 66-76.

Figure 7. Lessons from Confidence-Building Measures in Biological Weapons. (cont.)

PROSPECTS FOR THE DEVELOPMENT OF CBMs FOR CYBER WEAPONS

We can already identify many facets of weapons control regimes that are being implemented or discussed in relation to cyber warfare. Figure 8 spells out steps that have already been taken toward the implementation of confidence-building measures in cyberspace.

1998:

- Russian Federation introduces draft resolution to UN, "Developments in the field of information and telecommunications in the context of international security."

2000:

- Stanford University Center for International Security and Cooperation recommends a multilateral treaty to deal with cybersecurity and proposes the creation of an international agency with regulatory authority.

2001:

- Council of Europe Convention on Cybercrime includes provision that signatory states establish a hotline for coordinating mutual responses, provides for periodic consultations of parties.
- Russia proposes convening a UN group of governmental experts (GGE) on developments in the field of information and communications.

2003:

- Publication of White House "National Strategy to Secure Cyberspace."

2004:

- First UN group of government experts (GGE) meets to talk about threats in cyberspace. UN Secretary General admits in 2005 that no consensus was reached.

2006:

- Joint Staff initiates efforts to develop a "National Military Strategy for Cyberspace Operations."
- U.S. Air Force initiates provisional Cyber command.

Figure 8. Timeline of Confidence-Building Measures in Cyberspace.

2007:

- Cyberattacks on Estonia.

2008:

- International Telecommunications Union convenes World Summit on Information Society. Calls on ITU to facilitate the building of confidence and security in the use of information and communications technologies.
- NATO issues Draft Policy on Cyber Defense: creation of NATO"S Computer Incident Response Capability (NCIRC); Cyber Defense Management Authority (CDMA); NATO Cooperative Cyber Defense Center of Excellence.
- President Bush issues National Security Presidential Directive (NSPD) 54, Comprehensive National Cybersecurity Initiative, and spelling out role for Department of Homeland Security in defending domestic national critical infrastructure.
- Cyber attacks occur as part of Russian-Georgian War.

2009:

- Russia creates agreement with Shanghai Cooperation Organization (SCO) on sharing resources for information security.
- Rumored establishment of Russian "information troops."

2010:

- Discovery of Stuxnet virus.
- U.S. Cyber Command is officially established.

2011:

- China, Russia, Tajikistan and Uzbekistan introduce draft UN General Assembly Resolution, "an International Code of Conduct for Information Security."

Figure 8. Timeline of Confidence-Building Measures in Cyberspace. (cont.)

- Russia publishes Convention on International Information Security.

2012:

- Publication of Tallinn Manual on the International Law Applicable to Cyber Warfare.
- United Nations Institute for Disarmament Research holds inaugural Cyber Security Conference on "The Role of Confidence-Building Measures in Assuring Cyber Stability."

2013:

- Organization for Security Co-operation in Europe (OSCE) publishes initial set of confidence-building measures for cyberspace (Decision 1106), stressing that states should voluntary provide their views of cyber warfare and meet voluntarily to reduce risks of misperception.
- U.S. and Russia agree on bilateral activities for confidence-building in cyberspace, including a hotline between CERTs; direct communications link between U.S. Department of State and Ministry of Defense in Moscow; direct communications link between U.S. Cybersecurity Coordinator and Russian Deputy Secretary of the Security Council; creation of a bilateral working group on threats.
- United Nations group of government experts (UN GGE) proposes recommendations for CBMs in cyberspace, including a larger role for the UN in coordinating these measures. Members also voice agreement on Seoul Framework, which states that international law does apply in cyberspace.
- President Obama releases 2013 Cybersecurity Executive Order requiring the National Institute of Standards and Technology (NIST) to lead in developing a cybersecurity framework of standards and best practices for protecting critical infrastructure and directing regulatory agencies to determine the adequacy of current requirements and their authority to establish additional requirements to address risks.

2014:

- NIST Releases Cybersecurity Framework Version 1.0.

Figure 8. Timeline of Confidence-Building Measures in Cyberspace. (cont.)

CONCLUSION

As this report has shown, the development of confidence-building measures for the purposes of reducing cyber conflict is challenging. Because technology in the field of cyber warfare is advancing rapidly and in unpredictable ways, it is difficult to predict what sorts of issues might arise in the future or what sorts of measures might ultimately offer the most utility in terms of stemming conflict. However, it is clear that at the moment, there are certain elements in the field of cyber warfare that are lacking and need to be created and addressed prior to going forward.

First, the U.S. Government needs to take a leading role in starting a conversation about the ethics of cyber warfare and cyber weapons. Such a conversation needs to include practitioners, ethicists, and academics, as well as military personnel. Practitioners in particular need to be encouraged to think about their own statement of purpose, or what it means to be an individual or a community engaged in the production of new research in this field. Grants could be provided for the writing and production of textbooks in this area, and universities could be encouraged to include conversations about cyber ethics in introductory and graduate-level engineering and computer science courses.

Next, progress will not be made in the development of cyber confidence-building measures without the active and prolonged engagement of practitioners from academia and the private sector, as well as government. The issues are too complex for traditional government administrators to ever satisfactorily master on their own, and progress is advancing too rapidly for anyone but a specialist to keep up.

Finally, the U.S. Government, including the military, needs to decide consciously how committed they are to the principle of transparency and information sharing in this vitally important defense sector. Decisions regarding what information will be shared in the future need to be made with a full awareness of both the costs and benefits of agreeing to transparency.

Once these issues have been addressed, we might envision a series of treaties that would lay out:

a. **An agreement regarding the responsibilities of all states to secure their own nation's computer systems**. In the United States, policymakers have already created a voluntary agreement, which asks both government agencies and private industries to: regularly file reports regarding the protocols they are using to secure their systems, regularly run checks on their own systems, and regularly participate in exercises to make sure that they are not vulnerable. Commercial sector responses are coordinated through the National Institute for Standards and Technology's Cyber Security Framework, while the responses of both public and private sector actors concerned with critical infrastructure are coordinated through the Department of Homeland Security's Critical Infrastructure Cyber Community C3 Voluntary Program.

Here, all parties rely on a shared understanding of the norms of so-called "cyber hygiene," which is defined as:

> steps that computer users can take to improve their cybersecurity and better protect themselves online. It may include reorganizing the IT infrastructure, hardware and devices; patching authorized software and removing unauthorized software; continuous monitoring, training and awareness; and formalizing existing informal information security controls.[85]

b. **An agreement requiring states to provide notification of incursions detected into their system and sharing of that information with others through their nation's Computer Emergency Response Teams (CERTs)**. Here, protocols might resemble those that national organizations like the U.S. Center for Disease Control follow in sharing information about unusual disease outbreaks with the World Health Organization. Here the question may be how much information national CERTs and computer security incident response teams are willing to share with international contacts, including adversaries, and what the security risks to their own infrastructure might be from sharing this information.

c. **Establishment of an agreement that ranked and classified cyber weapons[86] and the establishment of a standard for what it might mean to be "adequately prepared" to wage cyber warfare—or what an adequate number and variety of cyber weapons might be**. Here the involvement of specialists will be key, and the resulting decisions may again end up resembling those undertaken by virologists and epidemiologists who have created systems for classifying types of biological weapons. The biological weapons community relies here on the criteria developed by the U.S. Army in 1964, as well as the Critical Agent List, which is organized and disseminated by the Centers for Disease Control. This list provides a starting point for assessing dual-use technologies through classifying which diseases present the greatest threat and thus require the continual development of new responses. In addition, it provides the basis for the granting of clearances to researchers working in this field.[87]

d. **An agreement regarding ethical standards for the cyber community that would spell out which methods of propagation and types of cyber weapons were viewed as either morally or legally unacceptable**. Here, the U.S. Government should commit resources to the development of an ethical and professional society for those who work in the field of computer science. The goal should be the creation of a set of ethical standards, which researchers in this field might commit to and share, and which would cause them to define certain activities (such as the creation of malicious code) as contrary to the spirit of the profession. Here, one can consider the codes of ethics which the Society of Professional Journalists or the American Society for Public Administration have adopted as a model.

The challenges will come from the fact that the so-called "hacker code of ethics" already exists and is widely shared by those who work in this field. However, the hacker code includes provisions that are at odds with U.S. national security interests—with its libertarian ethic of making information as free and widely available as possible, along with its resistance to practices of surveillance. Currently, it is difficult to see how a hacker code and an ethics code that has security at its core could be reconciled, but establishing a conference for the establishment of a code of ethics, along with furnishing grants to those who study ethics, might provide a valuable starting point.

Clearly, the shared understanding among biologists that "those who work in the life sciences do not create agents of death" has been a compelling and necessary underpinning for the self-policing of the organization by its members. This understanding is

not merely American, but nearly universal among biologists and for this reason, a true international epistemic community can be said to exist. This has helped to guide scientific developments in this field and provides a valuable hedge against the development of biological and chemical weapons. Similarly, a practitioner's group in the field of computer science might play this field if they were supported in efforts to create conferences, research and a journal of cyber warfare ethics.

e. **Establishment of specific parameters requiring the reporting of research advances, and the establishment of standards regulating the types of cyber warfare exercises that would be permitted both by military and civilian (private sector) practitioners**. As noted earlier, the involvement of specialists themselves will be key in establishing joint understandings regarding how and when information about security vulnerabilities and new methods of both offensive and cyber warfare will be shared. In time, the cyber community may decide, as the biological research community has, that some types of information are too dangerous to be reported in regular academic channels in open source journals and websites. Similarly, practitioners themselves will likely have to decide what types of hacking exercises and targets are appropriate for training purposes and which are not. Here, the U.S. Government can likely be of assistance but is unlikely to be the main driving force in making these decisions.

f. **Annual reporting**. In the area of biological weapons, the U.S. State Department issues an annual compliance report to Congress that reports on its own ac-

tivities, as well as those observed in other countries.[88] Here, it is likely that a body like the National Institute on Standards and Technology or the Department of Homeland Security might be tasked with reporting on the state of U.S. cyber hygiene in both the private and public sectors, as well as calling attention to any new developments in the fields of cyber warfare that would be of interest to Congress for the purposes of regulation and oversight.

As this report has shown, an ethic regarding the utility of these weapons and a shared understanding of transparency will not develop overnight. In addition, these concerns will never be divorced from other concerns, including domestic political concerns, relationships between actors in the international system, and other types of military decisions regarding warfare. However, progress is possible. Establishing a shared ethic and set of norms will be a valuable first step.

ENDNOTES

1. Emily Goldman and John Arquilla, "Introduction," Emily Goldman and John Arquilla, eds., *Cyber Analogies*, Monterey, CA: Naval Postgraduate School, 2014, pp. 1-7, available from *hdl.handle.net/10945/40037*, accessed May 22, 2014.

2. See Myriam Dunn Cavelty, "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities," *Science and Engineering Ethics*, 2014, available from *DOI 10.1007/s11948-014-9551-y*, accessed May 13, 2014.

3. *Ibid*., p. 5.

4. Here we can consider James Wirtz' "The Cyber Pearl Harbor Analogy," Emily Goldman and John Arquilla, eds., *Cyber Analogies*, Monterey, CA: Naval Postgraduate School, 2014, pp. 7-15; and Michael S. Goodman, "Applying the Historical

Lessons of Surprise Attack to the Cyber Domain: The Example of the United Kingdom," Emily Goldman and John Arquilla, eds., *Cyber Analogies*, Monterey, CA: Naval Postgraduate School, 2014, pp. 15-26, available from *hdl.handle.net/10945/40037*, accessed May 22, 2014. In contrast, only a scant two sentences appear in the volume on the possible utility of applying a weapons analogy. Robert Axelrod suggests looking at the lessons from the Chemical Weapons Convention in his list of 37 possible analogies, which might be useful in understanding new developments in cyber warfare. See his "A Repertory of Cyber Analogies," Emily Goldman and John Arquilla, eds., *Cyber Analogies*, Monterey, CA: Naval Postgraduate School, 2014, pp. 108-118. Also see David J. Betz and Tim Stevens, "Analogical Reasoning and Cyber Security," *Security Dialogue*, Vol. 44, No. 2, 2013, pp. 147-164.

5. See, for example, William Banks, "The Role of Counterterrorism Law in Shaping ad Bellum Norms," *International Law Studies*, Vol. 89, 2013, pp. 157-197. These understandings also appear in the *Quadrennial Defense Review Report*, Vol. 20, Washington, DC: U.S. Department of Defense, 2010.

6. Here we can consider, for example, language that appears in "Sustaining U.S. Global Leadership: Priorities for the 21st Century," Washington, DC: U.S. Department of Defense, The Pentagon, 2012. The report references cyber conflict five times: In four instances, territorial metaphors are used. However, the report also makes reference to the proliferation of technology that reinforces the asymmetric nature of threat today. The report notes that our adversaries are able to use techniques like electronic and cyber warfare to complicate our operational calculus (p. 4). See also Barack Obama, "Sustaining U.S. Global Leadership: Priorities for Twenty-First Century Defense," Washington, DC: Department of Defense, 2012, available from *www.defense.gov/news/Defense_Strategic_Guidance.pdf,* accessed May 6, 2014.

7. Indeed, Margaret Wertheim describes thinking about cyberspace territory as an extension of older theological and legal concepts of space, tracing them back to medieval understandings. See Margaret Wertheim, *The Pearly Gates of Cyberspace: A History of Space from Dante to the Internet*, New York: W. W. Norton and Co., 1999.

8. John Perry Barlow, "A Declaration of the Independence of Cyberspace," Online, February 8, 1996.

9. These claims are detailed in Mary Manjikian: "From Global Village to Virtual Battlefield: The Colonizing of the Internet and the Extension of Realpolitik," *International Studies Quarterly*, Vol. 54, No. 2, June 2010, pp. 381-401. For an analysis of Russian territorial claims to cyberspace, see Douglas Carman: "Translation and Analysis of the Doctrine of Information Security of the Russian Federation: Mass Media and the Politics of Identity," *Pacific Rim Law and Policy Journal, 2002*, available from *hdl.handle.net/1773.1/757*, accessed May 8, 2014.

10. Abraham D. Sofaer, David Clark, and Whitfield Diffie, "Cyber Security and International Agreements," Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, Washington, DC: National Academies Press, 2010, p. 180, available from *nap.edu/catalog/12997.html,* accessed April 12, 2014.

11. Quoted in Tim Maurer, "Cyber Norm Emergence at the United Nations—An Analysis of the UN's Activities Regarding Cybersecurity," *Discussion Paper 2011-11,* Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011, p. 5.

12. John D. Negroponte and Samuel L. Palmisano, "Defending an Open, Global, Secure and Resilient Internet," *Independent Task Force Report No. 70,* New York: Council on Foreign Relations, 2014.

13. I have introduced the term "cyber territory" to distinguish the particular notion that a state may own part of cyberspace through claiming it as territory from the more general term "cyberspace" which refers only to the fact that events and agreements are taking place in cyberspace or virtual space rather than in real space. The ways in which international relations theorists think about territory in particular is described in John Agnew, "The Territorial Trap: The Geographical Assumptions of International Relations Theory," *Review of International Political Economy* Vol. 1, No. 1, 1994, pp. 53-80.

14. Sofaer *et al*.

15. Taken from P. K. Ghosh, "Maritime Confidence-building Measures in South Asia—The Case of India and Pakistan," *Insights*, No. 8, May 2008, p. 32.

16. A. Z. Hilali, "Confidence and Security Building Measures for India and Pakistan," *Alternatives: Global, Local, Political*, Vol. 30, 2005, pp. 191-222.

17. Anne Finger and Oliver Meier, "Confidence-Building on Tactical Nuclear Weapons, What's On the Table?" Hamburg, Germany: Institute fur Friedensforschung und Sicherheitspolitik, 2013.

18. The theory behind the development of confidence-building measures is spelled out in Raimo Vayrynen, "The European Cooperation and Security Process Security Dilemmas and Confidence-Building Measures," *Security Dialogue,* Vol. 16, No. 4, 1985, pp. 349-361.

19. See Frank Jacobs, "Peacocks at Sunset," *The New York Times*, July 3, 2012, available from *opinionator.blogs.nytimes.com/2012/07/03/peacocks-at-sunset/*, accessed May 12, 2014.

20. See Radha Kumar, "The Troubled History of Partition," *Foreign Affairs* Vol. 76, No. 1, January/February, 1997, available from *foreignaffairs.com/articles/52641/radha-kumar/the-troubled-history-of-partition*, accessed May 2, 2014.

21. "Maritime Confidence Building Measures in the South China Sea," Barton, Australia: Australian Strategic Policy Institute, September 27, 2013, available from *https//aspi.org.au/publications/special-report-maritime-confidence-building-measures-in-the-south-china-sea-conference*, accessed May 2, 2014.

22. Ronald J. Deibert, "Bounding Cyber Power, Escalation and Restraint in Global Cyberspace," *Internet Governance Papers*, No. 6, Toronto, Canada: Center for International Governance Innovation, October 2013, p. 12.

23. Hilali, p. 119.

24. See the somewhat pessimistic assessment put forth by T. Najmudheen and Farhana Kausar, "Importance of Confidence Building Measures in India-Pakistan Relationships: A South Asian Perspective," *Asia-Pacific Journal of Social Sciences,* Vol. 5, No. 1, 2013, pp. 61-91. See also Samarjit Ghosh, "Two Decades of Indo-Pak CBMs, A Critique from India," New Delhi, India: Institute of Peace and Conflict Studies, 2009.

25. Ghosh, p. 34.

26. Hilali, p. 218.

27. Sofaer *et al*., p. 185.

28. *Ibid*.

29. Sofaer *et al.,* p. 198.

30. Christopher Castelli, "US-Russian Cybersecurity Talks Face Uncertainty amid Ukraine Crisis," *Inside Cybersecurity*, March 13, 2014, available from *insidecybersecurity.com/Cyber-General/Cyber-Public-Content/us-russian-cybersecurity-talks-face-uncertainty-amid-ukrainian-crisis/menu-id-1089.html,* accessed May 2, 2014.

31. David A. Rickards, "No Air, Cyber Dependency and the Doctrine Gap," Newport, RI: U.S. Naval War College, Joint Military Operations Department, 2010.

32. Dorothy E. Denning and Bradley J. Strawser, "Active Cyber Defense, Applying Air Defense to the Cyber Domain," Emily Goldman and John Arquilla, eds., *Cyber Analogies*, Monterey, CA, Naval Postgraduate School, 2014, p. 72, available from *hdl.handle.net/10945/40037*, accessed May 22, 2014.

33. This debate is described in Peter Feaver and Kenneth Gears, "'When the Urgency of Time and Circumstances Clearly Does not Permit Redelegation in Nuclear and Cyber Scenarios," Emily Goldman and John Arquilla, eds., *Cyber Analogies*, Monterey, CA, Naval Postgraduate School, 2014, pp. 33-46.

34. Rickards, p. 8.

35. Denning and Strawser, p. 69.

36. Finger and Meier, p. 5.

37. For more on this parallel, see Matthew D. Crosston, "World gone MAD, How 'Mutually Assured Debilitation' is the Best Hope for Cyber Deterrence," *Strategic Studies Quarterly*, Spring 2011, pp. 100-117.

38. Dennis Fisher, "E.U. Petition Seeks to Restrict Export of 'Digital Arms'," *Threat Post*, October 31, 2013, available from *threatpost.com/eu-petition-seeks-to-restrict-export-of-digital-arms*, accessed May 12, 2014.

39. Council of Europe, *Convention on Cybercrime*, Budapest, and Hungary: Council of Europe, November 23, 2001, available from *conventions.coe.int/Treaty/en/Treaties/Html/185.htm*, accessed May 2, 2014.

40. These events are described in "You only Click Twice, FinFisher's Global Proliferation," *Citizen Lab*, March 13, 2013, available from *https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/,* accessed May 1, 2014.

41. Jennifer Granick and Mailyn Fidler, "Changes to Export Control Arrangement Apply to Computer Exploits and More," *Just Security Blog*, January 15, 2014, available from *justsecurity.org/5703/export-control-arrangement-apply-computer-exploits/*, accessed May 16, 2014.

42. Negroponte and Palmisano.

43. Deibert, 2013.

44. *Ibid*.

45. Specific codes of conduct are spelled out in "Biological Weapons and Codes of Conduct," Devon, UK: Exeter University, 2014 available from *projects.exeter.ac.uk/codesofconduct/Chronology*, accessed May 12, 2014.

46. Gregory Koblenz, *Living Weapons, Biological Warfare and International Security*, Ithaca, NY: Cornell University Press, 2009, p. 21.

47. Ellen Nakashima, "NSA Director Calls for Stronger Strategy to Deter Cyberattacks," *The Washington Post*, February 27, 2012, available from *www.washingtonpost.com/world/national-security/nsa-director-calls-for-stronger-deterrent-strategy-to-oppose-cyberattacks/2014/02/27/aabd3d92-9fd4-11e3-a050-dc3322a-94fa7_story.html,* accessed May 8, 2014.

48. Koblenz. Also see Jeanne Guillemin, *Biological Weapons, From the Invention of State-Sponsored Programs to Contemporary Bio-terrorism*, New York: Columbia University Press, 2005, p. 1.

49. Theodore Karasik, "Toxic Warfare," Washington, DC: Rand Corporation, 2002.

50. Filippa Lentzos, "Strengthening the Biological Weapons Convention Confidence-building Measures, Toward a Cycle of Engagement," *Bulletin of the Atomic Scientists*, Vol. 67, No. 3, 2011, pp. 26-33.

51. Koblenz, p. 74.

52. *Ibid*., p. 73.

53. See, for example, Kathleen M. Vogel and Christine Knight, "Analytic Outreach for Intelligence, Insights from a Workshop on Emerging Biotechnology Threats," *Intelligence and National Security*, 2014, available from *www.tandfonline.com/doi/pdf/10.1080/02684527.2014.887633,* accessed May 1, 2014.

54. See, for example, Jung-Yong Yeh, Jee-Yong Parik, Yun Sang Cho, and In-Soo Cho, "Animal Biowarfare Research, Historical Perspective and Potential Future Attacks," *Zoonoses and Public Health*, Vol. 59, No. 8, 2012, pp. 536-544. See also Florence J. Yuzon, "Deliberate Environmental Modification Through the Use of Chemical and Biological Weapons, 'Greening' the International Laws of Armed Conflict to Establish an Environmentally Protective Regime," *American University International Law Review* Vol. 11, No. 5, 1996, pp. 793-846.

55. Guillemin, p. 7.

56. Margaret Hallissy, *Venomous Woman*, Westport, CT, Greenwood Press, 1987, pp. 5-6.

57. Guillemin, p. 5.

58. Koblenz, p. ix.

59. Guillemin, p. ix.

60. Mark Wheelis, Lajos Rozsa, and Malcolm Dando, "Historical Context and Overview," Mark Wheelis, Lajos Rozsa, and Malcolm Dando, eds., *Deadly Cultures: Biological Weapons since 1945*, Cambridge, MA: Harvard University Press, 2006, pp. 1-8.

61. *Ibid*., p. 8.

62. Richard Price, "A Genealogy of the Chemical Weapons Taboo," *International Organization,* Vol. 49, No. 1, 1995, p. 78.

63. Kirk C. Bansak, "Managing Networks of Risk, A Tailored Approach to Iran's Biological Warfare Threat Potential." *Bulletin of the Atomic Scientists,* Vol. 67, No. 5, 2011, p. 71.

64. Mark Wheelis, Lajos Rozsa, and Malcolm Dando., eds., *Deadly Cultures, Biological Weapons since 1945,* Cambridge, MA: Harvard University Press, 2006, p. 45.

65. See, for example, Price, pp. 73-103.

66. Guillemin, p. 11.

67. Sofaer *et al*.

68. See also Arturo Casadevall, "The Future of Biological Warfare," *Microbial Biotechnology*, Vol. 5, No. 5, 2012, pp. 584-587.

69. Bansak, pp. 66-76.

70. United Nations, "Building Confidence," available from *www.unog.ch/bwc.cbms*, accessed May 18, 2014.

71. Angela Woodward, "Banning Biological Weapons, National Legislation in Africa," *African Security Review*, Vol. 14, No. 1, 2005, pp. 23-34.

72. *Ibid*., p. 24.

73. Committee on Effectiveness of National Biosurveillance Systems, *Biowatch and Public Health Surveillance, Evaluating Systems for the Early Detection of Biological Threats,* Washington, DC: National Academies Press, 2011.

74. Woodward, p. 24.

75. *Ibid*., p. 24.

76. This series of decisions is spelled out in Michael J. Selgelid, "Governance of Dual-use Research, An Ethical Dilemma," *Bulletin of the World Health Organization*, June 30, 2009, available from *who.int/bulletin/volumes/87/9/08-051383/en/*, accessed May 18, 2014. See also Raymond A. Zilinskas and Jonathan B. Tucker, "Workshop Report, Options for Limiting the Contributions of Open Scientific Literature to the Biological Weapons Threat," Monterey, CA: Monterey Institute of International Studies, Center for Nonproliferation Studies.

77. Michael Willrich, *Pox, An American History*, New York: Penguin Press, 2011.

78. Jack Beard, "The Shortcomings of Indeterminacy in Arms Control Regimes, The Case of the Biological Weapons Convention," *American Journal of International Law*, Vol. 101, No. 271, April 2007, pp. 271-321.

79. Koblenz, p. 107.

80. On possible threats to CBM developments in cyberspace, see Castelli.

81. Koblenz, p. 75.

82. Iris Hunger, "La Transparence Dans le Controle des Armes Biologiques" ("Transparency in the Control of Biological

Weapons"), *Securite Globale* (*Global Security*), Vol. 3, No. 17, 2011, pp. 117-132.

83. N. A. J. Taylor, Joseph A. Camilleri, and Michael Hamel-Green, "Dialogue on Middle East Biological, Nuclear and Chemical Weapons Disarmament, Constraints and Opportunities," *Alternatives: Global, Local and Political*, Vol. 38, No. 1, 2013, p. 79.

84. Hanis Haziqah, Md Hambali, Megan Hafizal, Megan Ramli, Noorliza Hamdan and Zalini Yunus, "Implementation of the Biological and Toxic Weapons Convention (BTWC) in Malaysia, Challenges, and the Way Forward," *Defence S&T Technical Bulletin*, Vol. 5, Issue 2, 2012, pp. 84-98.

85. Definition taken from "The IT Law Wiki," available from *itlaw.wikia.com/wiki/Cyber_hygiene*, accessed May 8, 2014.

86. See Trey Herr, "PrEP: A Framework for Malware and Cyberweapons," Report GW-CSPRI-20-14.2, Washington, DC: George Washington University, Cybersecurity Policy and Research Institute, March 12, 2014.

87. This classification system is described in Rebecca Katz, "Biological Weapons, A National Security Problem that Requires a Public Health Response," Working Paper 2001-04, Princeton, NJ: Princeton University, Office of Population Research.

88. Lentzos, p. 27.

U.S. ARMY WAR COLLEGE

Major General William E. Rapp
Commandant

*****

STRATEGIC STUDIES INSTITUTE
and
U.S. ARMY WAR COLLEGE PRESS

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven K. Metz

Author
Dr. Mary Manjikian

Editor for Production
Dr. James G. Pierce

Publications Assistant
Ms. Rita A. Rummel

*****

Composition
Mrs. Jennifer E. Nevil





FOR THIS AND OTHER PUBLICATIONS, VISIT US AT
http://www.carlisle.army.mil/

ISBN 1-58487-666-2
9 781584 876663
90000>

This Publication

SSI Website

USAWC Website