S. HRG. 115–181

CYBER STRATEGY, POLICY AND ORGANIZATION

HEARINGS

BEFORE THE

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

MARCH 2 AND MAY 11, 2017

Printed for the use of the Committee on Armed Services

Available via the World Wide Web: http://www.Govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
28–907 PDF WASHINGTON : 2019

COMMITTEE ON ARMED SERVICES

JOHN MCCAIN, Arizona, *Chairman*

JAMES M. INHOFE, Oklahoma	JACK REED, Rhode Island
ROGER F. WICKER, Mississippi	BILL NELSON, Florida
DEB FISCHER, Nebraska	CLAIRE MCCASKILL, Missouri
TOM COTTON, Arkansas	JEANNE SHAHEEN, New Hampshire
MIKE ROUNDS, South Dakota	KIRSTEN E. GILLIBRAND, New York
JONI ERNST, Iowa	RICHARD BLUMENTHAL, Connecticut
THOM TILLIS, North Carolina	JOE DONNELLY, Indiana
DAN SULLIVAN, Alaska	MAZIE K. HIRONO, Hawaii
DAVID PERDUE, Georgia	TIM KAINE, Virginia
TED CRUZ, Texas	ANGUS S. KING, JR., Maine
LINDSEY GRAHAM, South Carolina	MARTIN HEINRICH, New Mexico
BEN SASSE, Nebraska	ELIZABETH WARREN, Massachusetts
LUTHER STRANGE, Alabama	GARY C. PETERS, Michigan

CHRISTIAN D. BROSE, *Staff Director*
ELIZABETH L. KING, *Minority Staff Director*

CONTENTS

MARCH 2, 2017

MAY 11, 2017

CYBER STRATEGY AND POLICY

THURSDAY, MARCH 2, 2017

U.S. SENATE,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The committee met, pursuant to notice, at 9:40 a.m. in Room SH–216, Hart Senate Office Building, Senator John McCain (chairman) presiding.

Committee members present: Senators McCain, Inhofe, Wicker, Fischer, Rounds, Ernst, Perdue, Sasse, Strange, Reed, Nelson, McCaskill, Shaheen, Gillibrand, Blumenthal, Donnelly, Hirono, Kaine, King, Heinrich, Warren, and Peters.

OPENING STATEMENT OF SENATOR JOHN MCCAIN, CHAIRMAN

Chairman MCCAIN. Our first panel of witnesses is Keith Alexander, CEO and President of IronNet Cybersecurity; Dr. Craig Fields, Chairman of the Defense Science Board; Dr. Jim Miller, former Under Secretary of Defense for Policy; and Matthew Waxman, Professor of Law at Columbia University Law School.

Threats to the United States in cyberspace continue to grow in scope and severity, but our nation remains woefully unprepared to address these threats, which will be a defining feature of 21st century warfare.

This committee has not been shy about expressing its displeasure over the lack of policy and strategy for deterring, defending against, and responding to cyber attacks. Treating every attack on a case-by-case basis, as we have done over the last eight years, has bred indecision and inaction. The appearance of weakness has emboldened our adversaries, who believe they can attack the United States in cyberspace with impunity.

I have yet to find any serious person who believes we have a strategic advantage over our adversaries in cyberspace. In fact, many of our civilian and military leaders have explicitly warned the opposite. In short, this committee is well aware that bold action is required, and we will continue to apply the appropriate pressure to ensure that the new administration develops a cyber strategy that represents a clean break from the past.

Such a strategy must address the key gaps in our cyber, legal, strategic, and policy frameworks. That's the topic of today's hearing, which is part of this committee's focused oversight on cyber strategy and policy. Each of our witnesses brings a unique perspective to these issues.

General Alexander recently served on the Presidential Commission on Enhancing National Cyber Security. Given his extensive ex-

perience as Director of the National Security Agency and the first commander of the United States Cyber Command, we welcome his insights and guidance as we seek to ensure that our policies, capabilities, and the organization of the Federal Government are commensurate with the cyber challenges we face.

Dr. Fields and Dr. Miller have been involved with the Defense Science Board's Task Force on Cyber Deterrence, which was established in October of 2014 to evaluate the requirements for effective deterrence of cyber attacks. We're pleased that the Defense Science Board has completed its evaluation, and we urge the new administration to immediately focus its attention on deterrence in cyberspace, which requires a comprehensive strategy for imposing costs on those seeking to attack our country.

Cyber also involves complex but highly consequential legal questions, which is why I'm pleased that we have Mr. Waxman with us to shed some light on these challenges. For example, understanding what constitutes an act of war in cyberspace is a central question for any cyber policy or strategy, but it is one we as a government have failed to answer.

As cyber threats have evolved rapidly, our legal frameworks have failed to catch up, and this is just one of a long list of basic cyber questions we as a nation have yet to answer. What is our theory of cyber deterrence, and what is our strategy to implement it? Is our government organized appropriately to handle this threat, or are we so stovepiped that we cannot deal with it effectively? Who is accountable for this problem, and do they have sufficient authorities to deliver results? Are we in the Congress just as stovepiped on cyber as the executive branch such that our oversight actually reinforces problems rather than helping to resolve them? Do we need to change how we are organized?

Meanwhile, our adversaries are not waiting for us to get our act together. They're defining the norms of behavior in cyberspace while reaction in the United States is in a reactive crouch. We have to turn this around and ensure cyber norms reflect the values of a free and open society and do not undermine our national security.

Cyber may be one of the most consequential national security challenges in a generation, and it will not grow easier with time. Our adversaries now believe that the reward for attacking the United States in cyberspace outweighs the risk. Until that changes, until we develop a policy and strategy for cyber deterrence, until we demonstrate that an attack on the United States has consequences, cyber attacks will grow more frequent and more severe. This is the urgent task before us, and that's why this series of hearings is so critical.

I thank each of our witnesses for appearing today, and I look forward to their testimony.

Senator Reed?

STATEMENT OF SENATOR JACK REED

Senator REED. Thank you very much, Mr. Chairman. I want to thank you for holding this very timely and incredibly important hearing.

I want to welcome our distinguished panelists. Gentlemen, your service to the nation is deeply appreciated.

I think the Chairman realized that General Alexander and I were both going to be here, so he called for reinforcements from the Naval Academy. We have midshipmen, but we can handle it.

As the Chairman has indicated, this is an incredibly complex and diverse set of issues, each of which might merit a separate hearing. Indeed, I would concede in the future we have additional hearings on these topics. But we're asking for comments on the President's Commission on Enhancing National Cyber Security. Secretary Carter's Multiple Defense Science Board studies on cyber resilience and deterrence, and Professor Waxman's research on the international law aspects are part of this very complicated issue.

Each of these important projects seek to help the United States define a coherent and effective cyber policy and strategy. Your presence today will help us put these pieces together in a much more effective and thoughtful way. Thank you.

Professor Waxman rightly observes that international law governing actions in cyberspace is an important guide to behavior in international law and has inherent ambiguities and develops slowly in new areas like cyber. However, Professor Waxman nevertheless urges that U.S. policy draw sharper red lines than exist today, a recommendation clearly in line with the views of our other witnesses who emphasize the urgency of improving our deterrence and defensive capabilities.

One important element of Professor Waxman's statement is the principle of sovereignty in international law. In the physical world, international law does not allow the aircraft to transit through our nation's airspace without permission, nor is it permissible to take military actions in a territory of non-belligerence. By analogy, would this mean that it would be legal to send a cyber weapon to a distant target through networks of other sovereign nations without their permission? Would it be illegal to take down a Syrian jihadist website hosted on a server that is in South Africa without the host nation's permission?

This committee has been asking these questions at least since General Alexander was nominated to lead the newly-established Cyber Command seven years ago. I would be interested in hearing each of the witnesses' views on these critical issues and more.

The Defense Science Board Task Force on Cyber Deterrence that Dr. Miller co-chaired makes a noteworthy recommendation directly pertinent to cyber attacks, such as the Russian intervention in our election last year. This task force report recommends that a key component of cyber deterrence is a development by the United States of capabilities to conduct what I will call information operations against the most valued assets or relationships of the leadership of a country that conducts a cyber attack on us. The report specifically cites Russia, Iran, North Korea, and China.

Dr. Miller, I'm interested in concrete examples of these most valued assets or relationships and what might be done to hold them at risk and what goal that accomplishes.

The recommendation to develop a capability to conduct information operations is an important one. However, I would note that we currently have very limited capabilities for mounting effective information operations that are sought and called for in this report. The report calls for assigning this responsibility to Cyber Com-

mand, but the cyber mission forces were built for a different role. They were built for defending networks against intrusion and for penetrating and disrupting others' networks, but not for conceiving and conducting operations involving content or cognitive manipulation.

Other organizations are currently assigned the responsibility for information operations, but they have been focused on supporting military forces in combat at the operational and tactical levels, not on strategic objectives. I look forward to hearing our witnesses' perspectives on specific steps to achieve this important capability both within and across the government.

Once again, Mr. Chairman, let me thank you for calling this incredibly important hearing. Thank you.

Chairman MCCAIN. Thank you.

As the members know, there's a vote that will begin at 10 o'clock. Usually we just kind of keep the hearing going, but I feel that this hearing is so important that maybe we'll wait until there's about 5 minutes left in the vote, in the first vote, take a brief recess, and come back after the second vote. I just think that the issue wants us to hear the full testimony.

So we will begin with you, General Alexander. Welcome back. I know how much you look forward to appearing before us again.

STATEMENT OF GENERAL KEITH B. ALEXANDER, USA, RETIRED, CEO AND PRESIDENT, IRONNET CYBERSECURITY

General ALEXANDER. Chairman McCain, Ranking Member Reed, members of the committee, it's an honor and privilege to be here. I provided a written statement and would ask that that be included in the record.

I want to address some of the things, Chairman, that we saw on the President's Commission on Enhancing National Cyber Security, and give you my insights on the path ahead, and it will address some of the statements that both you and Ranking Member Reed made.

First, I agree, our nation is woefully unprepared to handle cyber attacks in government and in the commercial sector, and this came out loud and clear in the Commission's hearing. There's a lack of policy, strategy, understanding of roles and responsibilities, and of rules of engagement. It requires a comprehensive architecture if we are to successfully defend this nation against a cyber attack. That architecture does not exist. While there are rules and laws in place that would allow it to exist, it doesn't exist today.

So the honor of sitting on that Commission was to identify and address some of these problems and push them forward for the next president, now President Trump and this administration to take on.

I want to give you some insights why I made those statements and what's in that commission report that we have.

First, if you look at technology and the way technology is advancing, it's doubling every two years. The amount of unique information that's being created doubles every year, which means this year we'll create more unique information than the last 5,000 years combined.

What that means for all of us is the rate of change in technology is going so fast that our IP and cyber personnel are having a very difficult time staying up. At the same time, as you identified, Chairman, the attacks are getting greater. If you think just 10 years ago the iPhone was created, and that's when the first nation-state attack occurred from Russia on Estonia, and then in 2008 from Russia on Georgia, and in 2008 we saw the penetration into the Defense Department networks that led to the creation of Cyber Command. In 2012 we saw the destructive attack against Saudi Aramco, and that was followed by 350 disruptive attacks on Wall Street, and it's getting worse.

Over the last three months we've seen destructive attacks on Saudi Arabia by Iran, and we are not prepared as a nation to handle those. Our industry and government are not working together. My experience in the last three years of being a civilian is that industry does want to work with government, but we haven't provided the relationships, and the roles and responsibilities of the different departments are not well understood. So I'll give you my insights of how those roles should be.

First, we have to have a government-industry partnership. If we think about the attack on Sony, the question is should Sony have been allowed to attack back. The answer we would come up with is no, because if Sony attacks back and the North Korean government thought that was an attack by our government, and it started a land war on the Korean Peninsula, we would all say that's industry starting a war; that's a government role and responsibility.

If it's the government's role and responsibility, how does the government do it, and who does it?

Senator Reed brought up the forces that we put in Cyber Command. We developed those forces to defend this country and our networks and provide offensive capabilities. In the last hearing we had a year ago, one of the statements that we jointly made was we should rehearse that. We should practice between key industry sectors, the energy sector, the financial sector, health care, the Internet service providers, and government on how we're going to defend this nation, and we should just do that, and we have failed to do that. I think that's one of the things that this committee can help push.

It's my opinion that the role and responsibility, as articulated in the Federal Roles and Responsibilities in Cyberspace, for defending this nation rests with the Defense Department. It's stated there. It's clearly to defend this country. Yet, when we talk to all of the departments about roles and responsibilities, it was clear that that was mixed up because we talked about different levels of roles and responsibilities, whether it was incident response, the role that DHS [Department of Homeland Security] would have, by defending the nation.

So we have to have, in my opinion, exercises and training where we bring the government, Congress, the administration, and industry together and practice this so we can all see how we're going to defend this country.

I believe that in doing that, the technology exists. More importantly, it's been my experience that industry wants to work with

government to help make this happen, and this is an opportunity for our government to stand together and do this.

One of the comments that I heard during the commission was it's too hard, there's too much data, and I brought out—and you would have been proud of this, Chairman McCain. I brought out the Constitution that I've read multiple times, and I said, well, here it says for the common defense. It doesn't say for the common defense unless it's too hard. It says we created this government, us, for the common defense of this nation, and we aren't doing that job.

That doesn't mean that we pay for industry doing their part. I think industry is more than willing to pay their part. But we in the government must help industry do it, especially when a nation-state attacks us.

So I think there is a way to overcome the lack of a strategy by creating a framework, setting up those roles and responsibilities, and the rules of engagement, and we ought to get on with it.

Thank you very much, Mr. Chairman.

[The prepared statement of General Alexander follows:]

PREPARED STATEMENT BY GENERAL (RETIRED) KEITH B. ALEXANDER [1]

Chairman McCain, Ranking Member Reed, Members of the Committee: thank you for inviting me to discuss cyber strategy and policy with you today, and specifically for asking this panel to engage in a dialogue with this Committee about how we might provide for the common defense of the nation in cyberspace. I plan to speak candidly about these issues, including the current organizational construct for cybersecurity within the federal government, the need for joint cyber defense capabilities and operations between the public and private sector, and the insights and recommendations of the Commission for Enhancing National Cybersecurity, of which I was a member.

Before I begin my testimony, I want to note the leadership, Mr. Chairman, that you and the Ranking Member are demonstrating by taking the time to look at how we might architect the federal government to deal with the reality of the threats that our nation faces in this rapidly-evolving, technology-driven, highly-networked global environment. The series of hearings focused on the future of warfare, global cyber threats, and cyber strategy and policy that you and the Ranking Member continue to chair will help ensure the security of our nation and allies for many decades going forward.

Mr. Chairman, we must fundamentally rethink our nation's architecture for cyber defense. We must recast the way we think of the respective roles and responsibilities of the government and private entities, bringing a new jointness to our work in cyber defense. We must develop a cadre of trained professionals that provides the public and private sectors a collective technical edge.

Overall, Mr. Chairman, I am concerned that as a nation, we have not made the key decisions necessary to put in place the foundational capabilities, provide the right authorities, and assign the critical responsibilities that are necessary to properly protect our nation in this new domain. I believe the cybersecurity Executive Order will be a key step in addressing some of these issues. In addition, I think it is critical that Congress, the White House, and the private sector work closely together to address the critical gaps that we face today.

For over 200 years, our Constitution has made clear that one of the core goals of the federal government is to provide "for the common defense." [2] Today, that common defense and the needed partnership between public and private sector is clearly lacking.

During my almost 40 years of service, it was an honor and privilege to work side-by-side with those who worked tirelessly to defend our nation. We worked hard to put in place the capabilities and to build the forces and structures needed to provide

[1] GEN (Retired) Keith Alexander is the former Commander, United States Cyber Command and Director, National Security Agency. Currently, he is the President and CEO of IronNet Cybersecurity and recently completed service as a member of the President's Commission on Enhancing National Cybersecurity.

[2] U.S. Const., preamble (emphasis added).

for the physical defense of our nation—both within our borders and abroad—and to do the same in cyberspace. Within the Department of Defense (DOD) alone, we fundamentally re-architected the way that the National Security Agency operated and created a key component of our nation's cyber defense, the U.S. Cyber Command.

In 2012, then-Secretary of Defense Leon Panetta made clear that the policy of the U.S. Government was that "the Department [of Defense] has a responsibility not only to defend DOD's networks, but also to be prepared to defend the nation and our national interests against an attack in or through cyberspace."[3] At that time, it was clear that in order to make our overall national cyber architecture truly defensible, we needed to establish a shared understanding of our respective roles and responsibilities, first within the government, then between the government and the private sector.

Initially, we worked closely with our colleagues in other agencies across the government to put in place a workable structure for sharing authorities and assigning responsibilities at the national level. Indeed, by one count, it took 75 drafts to obtain an agreement on a single slide regarding the national division of responsibilities for cybersecurity.[4]

At the end of that process, we assigned the responsibilities as follows: The Justice Department would, among other things, "[i]nvestigate, attribute, disrupt, and prosecute cyber crimes; [l]ead domestic national security operations; [and] [c]onduct domestic collection, analysis, and dissemination of cyber threat intelligence;" Department of Homeland Security (DHS) would, among other things "[c]oordinate the national protection, prevention, mitigation of, and recovery from cyber incidents; [d]isseminate domestic cyber threat and vulnerability analysis; [and] [p]rotect critical infrastructure;" and DOD would "[d]efend the nation from attack; [g]ather foreign threat intelligence and determine attribution; [and] [s]ecure national security and military systems."[5] Moreover, the "bubble chart," as this document was called, assigned the following lead roles: DOJ: investigation and enforcement; DHS: protection; and DOD: national defense.[6]

The position that DOD has the lead for national defense in cyberspace has been reiterated in both the 2014 Quadrennial Defense Review as well as the 2015 DOD Cyber Strategy, the latter of which also highlights the critical role that private sector entities must take in protecting themselves against threats in cyberspace.[7]

---

[3] *See* Department of Defense, *Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City* (Oct. 11, 2012), available online at *<http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136>*.

[4] *See* Department of Defense Information Operations Center for Research and Army Reserve Cyber Operations Group, *Cyber Endeavor 2014: Final Report—When the Lights Go Out,* at 5 (June 26, 2014), available online at *<https://my.nps.edu/documents/105372694/0/Cyber Endeavour 2014 - Final Report - 2014–08–13.pdf>* ("The need to define these partnerships and relationships [] led the Government and U.S. Federal Cybersecurity Operations Team to define their national roles and relationships as highlighted in Figure 1, which is commonly referred to as the 'Bubble Chart.' There were seventy-five (75) versions made of this chart before all parties agreed on how this works, and it was powerful and important just to get an agreement.")

[5] *See id.* at 6, Fig. 1.

[6] *See id.*

[7] *See* Department of Defense, *2014 Quadrennial Defense Review* at 14–15, available online at *<http://archive.defense.gov/pubs/2014_Quadrennial_Defense_Review.pdf>* ("The Department of Defense will deter, and when approved by the President and directed by the Secretary of Defense, will disrupt and deny adversary cyberspace operations that threaten U.S. interests. To do so, we must be able to defend the integrity of our own networks, protect our key systems and networks, conduct effective cyber operations overseas when directed, and defend the Nation from an imminent, destructive cyberattack on vital U.S. interests."); Department of Defense, *2015 Department of Defense Cyber Strategy* at 5 (Apr. 15, 2015), available online at *<http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DOD_CYBER_STRATEGY_for_web.pdf>* ("If directed by the President or the Secretary of Defense, the U.S. military may conduct cyber operations to counter an imminent or on-going attack against the U.S. Homeland or U.S. interests in cyberspace. The purpose of such a defensive measure is to blunt an attack and prevent the destruction of property or the loss of life . . . .As a matter of principle, the United States will seek to exhaust all network defense and law enforcement options to mitigate any potential cyber risk to the U.S. Homeland or U.S. interests before conducting a cyberspace operation. The United States government has a limited and specific role to play in defending the nation against cyberattacks of significant consequence. The private sector owns and operates over ninety percent of all of the networks and infrastructure of cyberspace and is thus the first line of defense. One of the most important steps for improving the United States' overall cybersecurity posture is for companies to prioritize the networks and data that they must protect and to invest in improving their own cybersecurity. While the U.S. Government must prepare to defend the country against the most dangerous attacks, the majority of intrusions can be stopped through relatively basic cybersecurity investments that companies can and must make themselves.")

While it may be clear that as a policy matter that DOD has the responsibility for defending the nation from nation-state attacks, the reality is that today U.S. Cyber Command lacks the clear authorities and rules of engagement to make this policy effective, even though it continues to build the forces and capabilities necessary to do so. It is critical that we work together, as a nation, to provide these authorities and rules of engagement now, when things are relatively calm, rather than seeking to identify and create them during a crisis. Mr. Chairman, I know that you and the Ranking Member have both taken the lead on working this effort, and I stand ready to assist you as needed.

While the primary responsibility of government is to defend the nation, the private sector also shares responsibility in creating the partnership necessary to make the defense of our nation possible. Neither the government nor the private sector can capably protect their systems and networks without extensive and close cooperation. The private sector controls most of the real estate in cyberspace, particularly when it comes to critical infrastructure and key resources,[8] and the notion that government might have control over, or even a constant, active defensive presence on these private systems and networks, is simply not something that our nation seeks today. Thus, given our current cyber architecture, if we are to create a truly defensible cyber environment, the government and the private sector must work closely together.

Consequently, the most important thing the government can do is to build connectivity and interoperability with the private sector. This is not simply connectivity and interoperability on a technology level, but on a policy and governance level. To that end, the Commission recommended the creation of a National Cybersecurity Public-Private Partnership (NCP3).[9] This entity, as set forth in Commission's report, would serve the President directly, reporting through the National Security Advisor and would function as "a forum for addressing cybersecurity issues through a high-level, joint public-private collaboration."[10] Part of the NCP3's key function would be to "identify clear roles and responsibilities for the private and public sectors in defending the nation in cyberspace," including addressing critical issues like "attribution, sharing of classified information . . . [and] an approach—including recommendations on the authorities and rules of engagement needed—to enable cooperative efforts between the government and private sector to protect the nation, including cooperative operations, training, and exercises."

In line with this recommendation, the Commission also recommended that "[t]he private sector and Administration [] launch a joint cybersecurity operation program for the public and private sectors to collaborate on cybersecurity activities in order to identify, protect from, detect, respond to, and recover from cyber incidents affecting critical infrastructure."[11] Empowering such joint efforts is critical to ensuring our long-term national security in cyberspace. As the Commission indicated, "[k]ey aspects of any collaborative defensive effort between the government and private sector [will] include coordinated protection and detection approaches to ensure resilience; fully integrated response, recovery, and plans; a series of annual cooperative training programs and exercises coordinated with key agencies and industry; and the development of interoperable systems."[12] Having such mechanisms in place well ahead of crisis is critical so that public and private sector entities can jointly train and exercise these rules of engagement and mitigate any potential spillover effects on ongoing business or government activities. Implementing these two Commission recommendations are amongst the most important things we might do as a nation in the near-term.

Finally, it is critical that the collaboration between the government and private sector is a two-way partnership. The government can and must do more when it comes to partnering with the private sector, building trust, and sharing threat information—yes, even highly classified threat information—at network speed and in a form that can be actioned rapidly. Building out a cross-cutting information sharing capability allows the government and private sector to develop a common operating picture, analogous to the air traffic control picture. As the air traffic control picture ensures our aviation safety and synchronizes government and civil aviation, the cyber common operational picture can be used to synchronize a common cyber de-

---

[8] *See,* e.g., Office of the Director of National Intelligence, Office of the Program Manager-Information Sharing Environment, *Critical Infrastructure and Key Resources,* available online at <*https://www.ise.gov/mission-partners/critical-infrastructure-and-key-resources*> ("The private sector owns and operates an estimated 85 percent of infrastructure and resources critical to our Nation's physical and economic security.").

[9] *Id.* at 14 (action item 1.2.1)

[10] *Id.* at 14–15.

[11] *Id.* at 15 (action item 1.2.2.)

[12] *Id.*

fense for our nation, drive decision-making, and enable rapid response across our entire national cyber infrastructure. This would provide a critical defensive capability for the nation.

The cyber legislation enacted by Congress last year is a step in the right direction; however, it lacks key features to truly encourage robust sharing, including placing overbearing requirements on the private sector, overly limiting liability protections, restricting how information might effectively be shared with the government, and keeping the specter of potential government regulation looming in the background.[13] Moreover, while the government has placed this responsibility with DHS today,[14] it is important to recognize the perception in industry is that DHS faces significant challenges in this area, in particular that it simply lacks the technical capabilities necessary to succeed.[15] More can be done here, and I stand ready to work with this Committee and others in Congress and the Administration as we seek a path forward on this important issue. As with the recommendations of the Commission above, I believe that implementing robust, real-time threat information sharing across the private sector and with the government would be a game-changer when it comes to cyber defense.

In sum, Mr. Chairman, I think much remains to be done to fully put our nation on a path to real security in cyberspace, and I am strongly hopeful for our future. With your leadership and that of the Ranking Member, working together collaboratively across the aisle and with the White House and key players in the private sector, we can achieve real successes in securing our nation in cyberspace.

Thank you for the opportunity to appear before this committee.

Chairman MCCAIN. Thank you for your testimony.

Dr. Fields?

STATEMENT OF DR. CRAIG I. FIELDS, CHAIRMAN, DEFENSE SCIENCE BOARD

Dr. FIELDS. Good morning, Chairman McCain, Ranking Member Reed, members of the committee. Jim, thank you for the microphone.

Dr. MILLER. It's a technology issue.

Dr. FIELDS. It's a technology issue.

We're here to talk about cyber deterrence. Jim and I have divided the presentation into two parts, and we ask that our written testimony be entered into the record.

What I want to do is to start by giving you a little view of the landscape of the Defense Science Board's study on cyber more generally, because there are actually a lot of pieces of the puzzle, and then offer to you eight principles that cyber has to comply with if we're going to be effective. These principles do not dictate the details of what to do in any circumstance, but they're like laws of physics; you have to comply. Then I'm going to turn it over to Jim and he's going to give you the main points, given time constraints,

---

[13] *See,* e.g., Jamil N. Jaffer, *Carrots and Sticks in Cyberspace: Addressing Key Issues in the Cybersecurity Information Sharing Act of 2015,* __S. Car. L. Rev. __(forthcoming 2017).

[14] See, e.g., Executive Order 13691, *Promoting Private Sector Cybersecurity Information Sharing* (Feb. 13, 2015), available online at <*https://www.whitehouse.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari*> ("The National Cybersecurity and Communications Integration Center (NCCIC), established under section 226(b) of the Homeland Security Act of 2002. . . shall engage in continuous, collaborative, and inclusive coordination with ISAOs on the sharing of information related to cybersecurity risks and incidents.").

[15] *See* Commission on Enhancing National Cybersecurity, *Testimony of Greg Rattray,* Director of Global Cyber Partnerships & Government Strategy, J.P. Morgan Chase (May 16, 2016) (describing DHS's six information sharing initiatives, as "too broad and [simply] not meet[ing] the need[] to enhance cyber defense"); *Testimony of Mark Gordon,* n. 13 *supra* (arguing that while tactically accelerating automating and systemizing threat indicator content with the government is a big vision, it is not a reality today); *see also* Jaffer, n. 14 *supra,* at __("DHS is generally seen as facing major challenges in capability in the cyber area and a number of other agencies, from DOD/NSA to FBI, are seen by industry as more capable, reliable, or secure.").

of our cyber deterrence task force. Then, of course, we'll enter into discussion later.

Again, in the interest of time, I'll be incredibly brief.

What is the DSB [Defense Science Board] going to do? Our study of cyber resilience, the main finding that's germane being that it's simply not possible to defend against a high-level threat. We can defend against mid- and low-level threats, but the high-level threats, like we could have from China or Russia, we have to deter. That's not a statement of criticism of our capabilities. That's true basically of any country because the means of deterring of defense are just not up to the means of offense at this point in time.

Cyber and cloud computing. How can DOD [Department of Defense] take advantage of the benefits of cloud computing without the risks?

Cyber defense management, some actionable recommendations for the Defense Department on how to basically optimally use financial resources, what are the most important things to do, what are the best practices in order to do cyber defense.

Cyber corruption of the supply chain. We get an awful lot of our micro-electronics from foreign sources. Sometimes what's inside is not what we think is inside. What do we do about that?

Cyber offense as a strategic capability. Right now we have good capabilities, but they're used episodically. How can we provide the President and the Congress with more of a strategic foundation so that when the unexpected arises, we're ready?

Acquisition of software. Parallel to a previous comment on micro-electronics, what we get is not always what we expect to get. How can we mitigate the risk?

Twenty-first century multi-domain. How do we harmonize kinetics, electronic warfare in cyber, in training, in authority, et cetera?

Then today's study, cyber deterrence. In addition, every one of our studies nowadays has a cyber component, be it unmanned vehicles or survival logistics or electronic warfare. I could go through a long list; I'm not going to. It pervades everything.

Just to give you a taste of the main features of what we've been doing, all of these studies contain what we call actionable recommendations for the Defense Department, and we think they're actually doable, versus just sort of high-level aspirations.

Part two, fundamental principles. These are the eight principles that I think we should all pay attention to as we address the issue of cyber deterrence.

Number one, you don't deter countries; you deter people. So you have to identify whose behavior you want to change, who you want to be deterred. If you can't do that, you can't get there. Trying to deter a mid- or low-level person, punishing a low-level person really doesn't work. You have to get to decision-makers, and they have to be deterred.

Number two and implied by the first, deterrence of an individual is a matter of an exercise of psychology, not of physics. Physics is a lot easier. Psychology is hard, especially when it crosses countries, is situationally dependent, and so on. But if we don't accept the fact that we're going to have to make judgments about what will deter individuals and it's a matter of psychology, we can't really make progress.

Number three, we should assume that people act on what they think is their self-interest, which is to say if we want to deter someone, we have to make their expected cost greater than their expected benefit. We can do that by reducing their expected benefit. We can do that by increasing their expected cost. There are notions and ideas for doing both, but that's the way you have to think about it. It has to be in scale. If the expected benefit is high, then if we want to deter we have to raise the expected cost considerably.

Number four and related, cyber deterrence does not have to be like for like. If you want to deter the use of cyber, you don't have to use cyber. You can use economic means or any number of other means. While we should act prudently, we should think broadly.

Number five, and again implied above, is U.S. responses to cyber attacks do not have to impose only a similar level of cost on an adversary. It can be greater. We have to obey the law. Mr. Waxman will address that, and I don't want to practice law without a license here. But we should be, again, flexible in our thinking even if we're prudent in our actions.

Number six, escalation. Escalation is always a concern, and it should be a concern. What we're typically facing is this: anything we do to deter contains some possibility of escalation. But not deterring carries a certainty of escalation. A possibility versus a certainty. But in other terms, we can have a certainty of a death of a thousand cuts or the possibility of escalation if we try to deter. So if we want to avoid all possibility of escalation, you can't deter. We have to accept the realities.

Some people think we live in a glass house and other countries don't. That's another whole discussion. That's just not true. Everybody, all major countries live in a glass house nowadays.

Seventh is chronology. It's a lot more effective to take deterring action quickly after something happens that you don't want to happen rather than waiting days, weeks, months, years. Chronology counts. That means you have to be prepared. The intelligence community has to collect the information in order to take action. CYBERCOM and other organizations have to be prepared to take action based on and using that information. The executive branch has to be able to orchestrate if it goes across various departments.

Number eight and last, credibility is critical. If no one believes that we're going to actually do what we say, then it doesn't matter what our capabilities are, it doesn't deter. Stating a red line and then letting people cross it with no consequence cuts down on our credibility. There may be good reasons for doing it, but that's a consequence. It cuts down on our credibility and hence our ability to deter, because the fact is we don't want conflict, we don't want war, we want a deterrent.

So again, these eight principles that I commend to you are not specific to this case or that. But as we plan for individual cases, I think we have to obey these as what citizens call boundary conditions. If we don't comply with these rules, we're not going to deter.

So at this point, I'll turn things over to Jim to talk about some of the specifics of our cyber deterrence task force.

Chairman MCCAIN. Thank you.

Dr. Miller, welcome back.

STATEMENT OF HONORABLE JAMES N. MILLER, MEMBER, DEFENSE SCIENCE BOARD AND FORMER UNDER SECRETARY OF DEFENSE FOR POLICY

Dr. MILLER. Thank you, Chairman McCain, Ranking Member Reed, members of the committee. It is an honor to be here again.

I'd like to start also by thanking Dr. Fields for allowing me to be the policy wonk among a number of technical gurus on the Defense Science Board. It's been a pleasure.

Finally I want to thank our task force members who are not here, and particularly my co-chair, Jim Gosler.

Our study on cyber deterrence with the Defense Science Board focused on the United States ability to deter cyber attacks such as Iran's distributed denial of service attacks that were conducted on Wall Street, as General Alexander mentioned, in 2012 to 2013; North Korea's cyber attack on Sony Pictures in 2014. We also covered what we described as costly cyber intrusions, such as the Chinese theft of intellectual property over the course of at least 10 years, and also the Russian hack of United States institutions which were intended to affect voter confidence and ultimately to affect the outcome of the recent United States presidential election.

In looking at the problem set, we found it useful to distinguish between three different sets of cyber challenges. The first is that major powers, Russia and China specifically, have a significant and growing ability to hold United States critical infrastructure at risk through cyber attack, and also a growing capability to hold at risk the United States military, and so to potentially undermine United States military responses. As Dr. Fields indicated, for at least the next decade the offensive cyber capabilities of these major powers are likely to far exceed the United States' ability to defend our critical infrastructure. At the same time, the United States military has a critical dependence on information technology, and these actors are pursuing the capability through cyber to thwart our military responses.

This emerging situation has the potential to place the United States in an untenable strategic position.

The second category of problem we looked at comes from regional powers such as Iran and North Korea. They have a growing potential to use either indigenous or purchased cyber tools to conduct catastrophic or significant attacks on United States critical infrastructure. For this problem set, the United States response capabilities need to be part of the tool kit, but they need to be added to what we do on cyber defenses and cyber resilience. It's no more palatable to allow the United States to be vulnerable to a catastrophic cyber attack by an Iran or a North Korea than it is to allow us to be vulnerable to a catastrophic nuclear attack by those actors.

Third, and the problem set with which we've had the most direct and immediate experience, is that a range of state and non-state actors have the capacity for persistent cyber attacks and costly cyber intrusions against the United States, some of which individually may be relatively inconsequential or only be one element of a broader campaign but which cumulatively subjects the nation, as Dr. Fields noted, to a death of a thousand hacks.

To address these three problem sets, the task force recommends three groups of initiatives. First, and consistent with what Chairman McCain said at the outset, the recommendation is that the United States Government plan and conduct tailored deterrence campaigns. A campaign approach is required to avoid piecemeal responses to cyber attacks and intrusions, and a tailored approach is needed to deal with both the range of actors and the range of potential scenarios that we may face. Clearly, for cyber deterrence, one size cannot fit all.

More specifically in this category, the task force recommended the following: update a declaratory policy that makes clear that the United States will respond to cyber attacks. The question is not whether; the question will only be how. Second, cyber deterrence campaign plans focused on the leadership of each potential adversary. Third——

Chairman MCCAIN. Excuse me. I don't mean to interrupt. Your first point, we haven't done that.

Dr. MILLER. That's correct, sir.

Chairman MCCAIN. Okay.

Dr. MILLER. The third element of this first section, adversary-specific playbooks are response options for cyber attacks to include both cyber and non-cyber, military and non-military responses. We can speak to why we need all those in the discussion if you'd like.

Fourth in this category, specific offensive cyber capabilities to support these playbook options, because one of the capabilities we certainly want in response to offensive cyber is offensive cyber. These capabilities need to be built out in a way that does not require burning intelligence axes when we exercise them.

Finally in this category, we recommend an offensive cyber capability Tiger Team be established consistent with Congress' direction for the Department to build Tiger Teams, and this one would look to develop options for accelerating acquisition, in particular offensive cyber capabilities.

The second broad category of recommendations was that the Defense Department develop what we described as a cyber resilient thin line of key United States strike systems. To credibly be able to impose unacceptable costs in response to cyber attack by major powers, Russia and China, the United States needs key strike systems—cyber, nuclear, and non-nuclear strike—to be able to function even after the most advanced cyber attack, and this is not a simple task. The task force made some specific recommendations and examples of long link strike systems to include—that's included in the prepared statement.

In support of this thin line cyber secure force, the task force recommended three actions in particular. First, an independent strategic cyber security program housed at NSA [National Security Agency] to perform top-tier cyber red teaming on the thin line of cyber long-range strike and nuclear deterrence systems. The model is similar to what we have with the SSBN [Submersible Ship Ballistic Nuclear] security program, which I know the committee is familiar with, looking at not just what could be done today but what could be done in future that has significant consequence.

A second component is a new best-of-breed cyber resilience program to identify the best security concepts in government and, im-

portantly, in the private sector as well, and to bring them to bear in a systematic way.

Third, an annual assessment of the cyber resilience of the U.S. nuclear deterrent, similar to what's done currently for the nuclear deterrent more broadly. This would be conducted by the commander of the Strategic Command, and the certification would go to the Secretary of Defense, to the President, and to the Congress.

The third broad category of recommendation the task force made, and the final category, is that the Department needs to continue to pursue and in some cases increase its efforts on foundational capabilities. That includes cyber attribution. It includes continued overall enhancement of the cyber resilience of the joint force. We put this as a lower priority than the so-called thin line capabilities, but it's important as well.

A third element here is continued and more aggressive pursuit of innovative technologies that can help reduce the vulnerability of U.S. critical infrastructure.

Fourth in this category is U.S. leadership, and define appropriate extended deterrence postures, and working with our allies and partners.

Finally, and last but certainly not least, is sustained and enhanced recruitment, training, and retention of a top-notch cyber cadre.

At the end of the day, from all the importance of technology in this area, the most important strategic advantage of the United States in cyber, as in other domains, is the incredible capabilities of our military, of our civilians, and of our private sector. DOD [Department of Defense] has taken some important steps to move forward on recommendations of this report over the course of its conduct, in parallel with its establishing its 133 cyber mission force teams. The recommendations which I've just described are intended to build on what the Department is doing to expand it and to accelerate it.

Again, thank you for the opportunity to testify today.

[The joint prepared statement of Dr. Fields and Dr. Miller follows:]

JOINT PREPARED STATEMENT BY DR. CRAIG FIELDS AND DR. JIM MILLER

INTRODUCTION

Chairman McCain, Ranking Member Reed, Members of the Committee. We are here today to discuss cyber deterrence.

By "cyber deterrence" we mean how to deter major cyber attacks on the United States, largely by foreign states, particularly great powers, but someday perhaps by capable non-states.

We want to begin by briefly introducing the Defense Science Board (DSB) and telling you about DSB's substantial agenda of studies regarding cyber. Then I have some fundamental principles to offer regarding how to be successful with cyber deterrence.

We will then turn to Jim Miller, co-chair with Jim Gosler of DSB's recent comprehensive study of cyber deterrence. He will present the major findings and recommendations of that investigation.

We would also like to underscore that the findings we reference are the Defense Science Board's and do not necessarily represent the perspectives, policies, or positions of the Department of Defense.

DEFENSE SCIENCE BOARD

For 60 years the Defense Science Board (DSB) has tackled highly unstructured, irksome and consequential problems for the Secretary of Defense that involve science and technology. And, inevitably, also strategy, tactics, management, rules of engagement and operational concepts as related to science and technology.

The members of DSB are senior executives from defense and commercial industry; retired flag officers; former senior officials from the Department of Defense, Department of State and the Intelligence Community; University professors, e.g. from MIT; CEOs of Federally Funded Research and Development Centers; National Laboratory Directors; and many members of the National Academy of Science and the National Academy of Engineering.

All with a strong background in science and technology; and with knowledge of DOD and national security matters.

DEFENSE SCIENCE BOARD STUDIES ON CYBER

DSB's first study on cyber dates from 1967, and to my knowledge that work was the first major investigation of the cyber threat with recommendations regarding how to mitigate and manage the threat.

Much more recently DSB has conducted a series of studies that in union provide a comprehensive set of findings and recommendations for the Department of Defense.

Cyber Resilience—recommendations for defense against low- and medium-level threats, and the recognition that we cannot adequately defend against high-level threats. Those must be deterred.

Cyber and Cloud Computing—How can DOD realize the tremendous benefits of economy of scale of cloud computing, while mitigating the risks of such shared and remote computing?

Cyber Defense Management—Insofar as cyber defense can be expensive—noting that lack of cyber defense can be considerably more expensive!—how should DOD optimally allocate its resources to provide the best protection?

Cyber Corruption of the Supply Chain—How can DOD mitigate the risk of malicious insertions in the microelectronics it buys?

Cyber Offense as a Strategic Capability—What does DOD have to do to ensure that the President has strategic options at hand to use prudently as unpredicted needs arise?

Acquisition of Software—In general how can DOD acquire software better, and in particular how can DOD mitigate the risk of cyber intrusion into our software?

Twenty-first Century Multi-Domain Integration—harmonizing cyber, kinetics and EW in all domains, in terms of capabilities, planning, training, C3 and so on

Cyber Deterrence—What needs to be done to effectively deter major cyber attacks on the United States?

In addition, cyber considerations play a role in almost all DSB studies. Most DOD systems contain computing, and most computing is vulnerable to cyber.

Thus, cyber considerations play a role in many DSB studies, including: information operations in gray zone conflicts; unmanned undersea vehicles; autonomous systems; countering autonomous systems; survivable logistics; electronic warfare (EW); ballistic and cruise missile defense; MILSAT and tactical communications; resilience of space capabilities; air dominance; and more.

SOME FUNDAMENTAL PRINCIPLES OF CYBER DETERRENCE

I would like to offer eight (8) fundamental principles that apply to cyber deterrence. The principles do NOT dictate exactly what to do in particular circumstances, but what to do in particular circumstances should conform to the principles.

First, we must deter specific people, specific individuals, the decision makers of foreign states, not countries. They decide whether or not to unleash a cyber attack on the United States. Trying to deter lower level individuals, e.g. 22-year-old hackers, mid-career civil servants, lower level military officers who are "following orders" is not effective.

Second, deterrence of an individual is an exercise in psychology, not physics. Physics is easier. It is an exercise in cross-cultural psychology, to make it more difficult. It is an exercise in situation-dependent psychology to make it more difficult still. Finally it is an exercise in psychology done from a distance insofar as the U.S. Government personnel charged with deterrence will likely have never met the individual we want to deter, or certainly have not spent sufficient time with them to develop deep understanding. That's the way it is. The implication is that we have to do the best we can, meaning be sure that the U.S. Government personnel charged

with cyber deterrence have access to the very best analysis regarding the individuals we want to deter.

Third, to deter a leader who might decide to order a cyber attack on the U.S. we need to hold at risk what they hold dear. We have to make their expected cost greater than their expected benefit. Where feasible at reasonable cost we should also decrease their expected benefit of a cyber attack on the U.S., e.g. with defense, protection, resilience or reconstitution of our critical infrastructure, but for the most capable adversaries, e.g. great powers, that is difficult.

Fourth, cyber deterrence does not have to be 'like for like', 'tit for tat'. Cyber does not have to be deterred with cyber. Deterrence could involve economic sanctions or other means.

Fifth, and related, U.S. responses to cyber attack do not have to aim to impose (only) a similar level of costs on the adversary as it imposed on the United States. While a response must meet legal requirements such as proportionality (avoiding unnecessary civilian loss of life or hardship), it must also be effective. That means imposing sufficient costs to deter future such attacks.

Sixth, escalation is always a concern and should always be a concern. All deterrence is accompanied by the possibility of escalation. But lack of deterrence is accompanied by the certainty of escalation. We are often faced with the alternatives of a certainty of 'a death of a thousand cuts' if we take no deterring action or the possibility of escalation if we take deterring action. There is no perfect solution but there is a constructive approach, namely to employ approaches to deterrence that are graded—do a little, see what happens, do a little more . . . —and reversible.

Seventh, chronology. It is considerably more effective to take deterring action sooner rather than later. Being prepared to act sooner carries some operational implications. Long in advance the Intelligence Community has to be tasked to collect the underlying information required to compose strategy, tactics and operational plans for deterring specific individuals. Long in advance the organizations that would be tasked with affecting deterrence, e.g. DOD, Treasury, need to have capabilities prepared and in place and compose the aforementioned strategy, tactics and operational concepts. And all this has to be orchestrated across various organs of the Executive Branch with effective communication with the appropriate elements of the Congress.

Eighth, credibility is a necessary enabler of deterrence. If the leader we want to deter does not believe we will act it is difficult to deter. Announcing 'red lines' and then overlooking offenses is not constructive.

To repeat, these eight principles do not dictate specific deterring actions for particular circumstances, but if we want to be effective in deterring major cyber attacks on the U.S. we should comply with the principles.

DEFENSE SCIENCE BOARD STUDY OF CYBER DETERRENCE

The DSB Cyber Deterrence Task Force was asked to consider the requirements for deterring cyber attacks against the United States and U.S. allies/partners, and to identify critical capabilities (cyber and non-cyber) needed to support deterrence, warfighting, and escalation control against highly cyber-capable adversaries. In conducting its work, the fifteen task force members received more than forty briefings from government, the national laboratories, academia, and the private sector.

Three Key Cyber Deterrence Challenges

The task force determined that the United States faces three distinct sets of cyber deterrence challenges.

First, major powers (Russia and China) have a significant and growing ability to hold United States critical infrastructure at risk via cyber attack—and to simultaneously use cyber to undermine U.S. military responses. The unfortunate reality is that for at least the next decade, the offensive cyber capabilities of these major powers are likely to far exceed the United States' ability to defend essential critical infrastructure. At the same time, they recognize that the U.S. military itself has an extensive dependence on information technology, and they are pursuing the capability to use cyber to thwart U.S. military responses. This emerging situation threatens to place the United States in an untenable strategic position.

Second, regional powers (such as Iran and North Korea) have a growing potential to use indigenous or purchased cyber tools to conduct catastrophic attacks on United States critical infrastructure. The U.S. Government must work with the private sector to intensify efforts to defend and boost the cyber resilience of U.S. critical infrastructure in order to avoid allowing extensive vulnerability to these nations. The United States would have a range of options to respond to any attack (cyber or other) by such nations. But these response capabilities must be additive to our de-

fenses. It is no more palatable to allow the United States to be held hostage to catastrophic attack via cyber weapons by such actors than via nuclear weapons.

Third, a range of state and non-state actors have the capacity for persistent cyber attacks and costly cyber intrusions against the United States, which individually may be inconsequential (or be only one element of a broader campaign) but which cumulatively subject the Nation to a "death by 1,000 hacks."

To address these three challenges, bolstering the U.S. cyber deterrence posture must be an urgent priority. The task force recommended that the Department of Defense and broader U.S. Government pursue three broad sets of initiatives.

1. *Plan and Conduct Tailored Deterrence Campaigns*

The United States cyber deterrence posture must be "tailored" to cope with the range of potential attacks that could be conducted by each potential adversary—including Russia, China, Iran, North Korea, and non-state actors including ISIS. And it must do so in contexts ranging from peacetime to "gray zone" conflicts to crisis to war. Clearly, for United States cyber deterrence (as with deterrence more broadly), one size will not fit all.

This requires, and the task force recommended:

- **Updated declaratory policy** that makes clear the United States will respond to *all* cyber attacks; the question will not be whether but how.
- **Cyber deterrence campaign plans** focused on the leadership of each potential adversary.
- **Adversary-specific "playbooks"** of response options to cyber attacks on the United States or its interests, ranging from low level hacks to major attacks, including cyber and non-cyber military responses, and potential non-military responses.
- **Specific offensive cyber capabilities** to support approved "playbook" options by holding at risk what is valued by adversary leaders; this should include capabilities that do not require "burning" intelligence accesses (sources and methods) when exercised.
- **An offensive cyber capability tiger team** to develop options to accelerate acquisition of offensive cyber capabilities to support deterrence, such as additional acquisition authorities for USCYBERCOM, and establishment of a small elite rapid acquisition organization.

The intention is not to create a "cookbook" approach to cyber deterrence. Rather it is to establish a clear policy and planning framework, to help drive prioritized cyber offensive capability development, and ultimately to give a range of good cyber and non-cyber options to support deterrence of—and as necessary response to—cyber attack.

2. *Create a Cyber-Resilient "Thin Line" of Key U.S. Strike Systems*

In order to support deterrence, the United States must be able to credibly threaten to impose unacceptable costs in response to even the most sophisticated large-scale cyber attacks. Meeting this requirement will require the Department of Defense to devote urgent and sustained attention to boosting the cyber resilience of select U.S. strike systems (cyber, nuclear, and non-nuclear) including their supporting critical infrastructures. In effect, DOD must create a second-strike cyber resilient "Thin Line" element of U.S. military forces to underwrite deterrence of major attacks by major powers.

This requires a **"thin line" cyber secure force** comprised of select elements of offensive cyber capabilities, select non-nuclear long-range strike systems, and all nuclear-capable systems. The Department should further enhance investments to protect and make resilient these capabilities. Examples of long-range non-nuclear strike systems that should be made highly resilient to cyber (and other non-nuclear attack) on an urgent basis include:

- A substantial number of general purpose attack submarines (SSNs) and guided missile submarines (SSGNs) armed with long-range strike systems (for example Tomahawk Land Attack Missiles (TLAMs));
- Heavy bombers armed with non-nuclear munitions capable of holding at risk a range of targets in standoff or penetrating mode (for example, extended range Joint Air to Surface Standoff Missiles (JASSM–ER) and Massive Ordnance Penetrators (MOPs));
- Supporting Command, Control, Communications and Intelligence, Surveillance and Reconnaissance (C3ISR) essential to support mission planning and execution; and
- Critical infrastructure essential to support platforms, munitions, C3ISR, logistical support, and personnel.

In support of this "thin line" cyber secure force, the task force recommended:

- **An independent Strategic Cyber Security Program (SCSP)** housed at the National Security Agency (NSA) to perform top tier cyber red teaming on selected offensive cyber, long-range strike, and nuclear deterrent systems. SCSP should look at current systems as well as future acquisitions before DOD invests in or employs new capabilities. The Navy's long-standing SSBN Security Program provides a useful model.
- **A new "best of breed" cyber resilience program** to identify the best available or emerging security concepts for critical information systems, drawing best practices and innovative ideas from across DOD and industry. This program should devise a broad portfolio of options to dramatically enhance cyber resilience of critical strike systems, ranging from emerging new technologies to the use of "retro-tech" such as electro-mechanical switches.
- **An annual assessment of the cyber resilience of the U.S. nuclear** deterrent, conducted by the Commander of U.S. Strategic Command, and provided to the Secretary of Defense, President, and Congressional leadership. including all essential nuclear "Thin Line" components (e.g., nuclear C3, platforms, delivery systems, and warheads). Commander USSTRATCOM should state his degree of confidence in the mission assurance of the nuclear deterrent against a top tier cyber threat.

3. *Pursue Foundational Capabilities*

In addition to the measures outlined above, the Department of Defense and the broader U.S. Government must continue to innovate in order to improve the posture of the United States regarding several foundational capabilities:

- **Cyber attribution;**
- **Continued enhancement of cyber resilience of the joint force**—though to a lesser level and as a lower priority than for selected long-range strike systems as discussed above;
- **Offensive and Defensive Cyber Security S&T:** U.S. research in both of these areas need to inform the other;
- **Innovative technologies** that can enhance the cyber security of the most vital U.S. critical infrastructure;
- **U.S. leadership in providing appropriate cyber "extended deterrence"** to allies and partners; and over time perhaps most importantly,
- **The sustained recruitment, training, and retention of a top-notch cyber cadre.**

Over the last several years, the Department of Defense has begun taking important steps to strengthen its cyber capabilities, including for example the establishment and initial operating capability of 133 cyber mission force teams. If implemented and sustained over time, the task force recommendations (outlined in this statement and described in much greater detail in the DSB report) will build from this prior work, and help guide the urgent actions needed to bolster deterrence of cyber attacks on the United States and our allies and partners.

Chairman MCCAIN. Thank you.

Mr. Waxman?

STATEMENT OF MATTHEW C. WAXMAN, LIVIU LIBRESCU PROFESSOR OF LAW, COLUMBIA UNIVERSITY LAW SCHOOL

Mr. WAXMAN. Chairman McCain, Ranking Member Reed——

Chairman MCCAIN. I apologize. I think we've only got 5 minutes left, so we'll take a brief recess. We have two votes, so it will probably be about 15 minutes, and we'll resume. Thank you.

[Recess.]

Chairman MCCAIN. We'll resume the hearing. I'm sure that other members will be coming back shortly, but we don't want to take too much time, and we want to resume with you, Mr. Waxman. Thank you.

Mr. WAXMAN. Thank you, Chairman McCain, Ranking Member Reed, committee members. I appreciate the opportunity to address some international law questions relevant to U.S. cyber strategy. These include when a cyber attack amounts to an act of war, as well as the international legal principle of sovereignty and how it

could apply to cyber activities. I also have a written statement that I hope can be made part of the record.

These are important questions because they affect how the United States may defend itself and what kinds of cyber actions the United States may take. They're difficult questions because they involve applying longstanding international rules developed in some cases over centuries to new and rapidly changing technologies and forms of warfare.

To state up-front my main point, international law in this area is not settled. There is, however, ample room within existing international law, including the U.N. Charter's thresholds, to support a strong cyber strategy and powerful deterrent. The United States should continue to exercise leadership in advancing interpretations that support its interests, including operational needs, bearing in mind that we also seek to constrain the behaviors of others.

It's important that the U.S. Government continue to refine and promote diplomatically its legal positions on these issues. Aside from the American commitment to the rule of law and treaty obligations, established rules help to influence opinions abroad, and they therefore raise or lower the cost of actions. Agreements on them internally within the government can speed decision-making, and agreements on them with allies can provide a basis for joint action.

With those objectives in mind, I'll turn first to the question whether a cyber attack could amount to an act of war. When should a cyber attack be treated legally the same way we would, say, a ballistic missile attack versus an act of espionage, or should cyber attacks be treated altogether differently with entirely new rules?

Different legal categories of hostile acts correspond to different legal options for countering them. The term "act of war" retains political meaning, but as a technical legal matter this term has been replaced by provisions of the United Nations Charter. Created after World War II, that central treaty prohibits the use of "force by states against each other," and it affirms that states have a right of self-defense against "armed attacks."

Historically, those provisions were interpreted to apply to acts of physical or kinetic violence, but questions arise today as to how they might apply to grave harms that can be inflicted through hacking and malicious code. Even if the cyber attack does not rise to those U.N. Charter thresholds—take, for example, the hack of a government system that results in large theft of sensitive data—the United States would still have a broad menu of options for responding to them; and even cyber attacks that do not amount to force or armed attack may still violate other international law rules.

However, a cyber attack that crosses the force or armed attack threshold would trigger legally an even wider set of responsive options, notably including military force or cyber actions that would otherwise be prohibited. In recent years the United States Government has taken the public position that some cyber attacks could cross the U.N. Charter's legal thresholds of force or armed attack. It is said that these determinations should consider many factors,

including the nature and magnitude of injury to people and property.

So at least for cases of cyber attacks that directly cause the sort of damage normally caused by, for example, a bomb or missile, the U.S. Government has declared it appropriate to treat them legally as one would an act of kinetic violence. Publicly, the United States Government usually provides only quite extreme scenarios, such as inducing a nuclear meltdown or causing aircraft to crash by interfering with control systems.

This approach to applying by analogy well-established international legal rules and traditional thresholds to new technologies is not the only reasonable interpretation, but it is sensible and can accommodate a strong cyber strategy. It is likely better than alternatives such as declaring the U.N. Charter rules irrelevant or trying to negotiate new cyber rules from scratch.

However, the United States Government's approach to date leaves a lot of gray areas. It leaves open how to treat some cyber attacks that do not directly and immediately cause physical injuries or destruction but that still cause massive harm. Take, for instance, a major outage of banking and financial services, or that weaken our defensive capabilities such as disrupting the functionality of military early warning systems. More clarity on this issue is important.

Although the act of war or armed attack question usually attracts more attention, I want to raise another important international law issue, and that's the meaning of sovereignty in cyber. This could have significant impact on offensive and defensive options, and I'm glad that Ranking Member Reed mentioned this.

Sovereignty is a well-established principle in international law. In general, it protects each state's authority and independence within its own territory. But sovereignty is not absolute, and its precise meaning is fuzzy. Because of the global interconnectedness of digital systems, including the fact that much data is stored abroad and constantly moving across territorial borders, questions could arise as to whether cyber activities, including U.S. offensive cyber actions or defensive cyber measures that occur in or transit third countries without their consent, might violate their sovereignty.

Now, as a policy matter, we have a strong interest in limiting infiltration and manipulation of our own digital systems, and it may usually be wise to seek consent from states that host digital systems that might be affected or used in cyber operations. However, it is my view that there is not enough evidence of consistent and general practice among states, or a sense of binding legal obligation among them, to conclude that the principle of sovereignty would prohibit cyber operations just because, for example, some cyber activities take place within another state or even have some effects on its cyber infrastructure without consent, especially when the effects are minimal.

I thank you very much for the opportunity to address the committee, and I look forward to your questions.

[The prepared statement of Mr. Waxman follows:]

PREPARED STATEMENT BY MATTHEW C. WAXMAN

Chairman McCain, Ranking Member Reed, members of the committee, and staff. I appreciate the opportunity to address this critical topic.

In discussing cyber policy and deterrence, I have been asked specifically to address some of the international law questions most relevant to cyber threats and U.S. strategy. These include whether and when a cyber-attack amounts to an "act of war," or, more precisely, an "armed attack" triggering a right of self-defense. I would also like to raise the issue of how the international legal principle of "sovereignty" could apply to cyber activities, including to the United States' own cyber-operations.

These are important questions because they affect how the United States may defend itself against cyber-attacks and what kinds of cyber-actions the United States may itself take. They are difficult questions because they involve international rules, developed in some cases over centuries, to deal with new and rapidly changing technologies and forms of warfare.

To state up-front my main points: International law in this area is not settled. There is, however, ample room within existing international law to support a strong cyber strategy, including a powerful deterrent. The answers to many international law questions discussed below depend on specific, case-by-case facts, and are likely to be highly contested for a long time to come. This means that the United States should continue to exercise leadership in advancing interpretations that support its strategic interests, including its own operational needs, bearing in mind that we also seek rules that will effectively constrain the behaviors of others. [1]

Before turning to some specific questions, let me say a few words about why international law matters here, and why it is important that the U.S. Government continues to refine, explain and promote diplomatically its legal positions on these issues. Besides American commitment to rule of law and treaty obligations, international law is relevant to U.S. cyber strategy in several ways. Established rules and obligations help influence opinions and shape reactions among audiences abroad, and they therefore raise or lower the costs of actions. They may be useful in setting, communicating and reinforcing "red lines," as well as for preserving international stability, especially during crises. Agreement on them internally within the government can speed decision-making. And agreement on them with allies can provide a basis for cooperation and joint action.

In approaching these legal questions, the U.S. Government also must think through what legal rules or interpretations it seeks to defend itself as well as how those legal rules might limit its authority to carry out its own cyber-operations. And, of course, the same rules and interpretations advanced by the United States may be used by other states to help justify their own actions.

With those objectives in mind, I will turn to some specific international legal questions.

First, it is sometimes asked whether a cyber-attack could amount to an "act of war." More broadly, how are cyber-attacks classified or categorized under international law? When should a cyber-attack be treated legally the same way we would treat a ballistic missile attack, for example, versus an act of espionage, or an act of economic competition? Or should actions carried out in cyberspace be treated altogether differently, with entirely new rules? One reason this matters is that certain broad categories of hostile actions are prohibited under well-established international law. Another reason is that how a hostile action is categorized under international law is relevant to what types and levels of defensive responses are permitted. That is, different legal categories of hostile acts correspond to different legal options for countering them.

The term "act of war" retains political meaning, usually to signify the hostile intent and magnitude of threat posed by an adversary's actions. As a technical legal matter, this term has been replaced by provisions of the United Nations Charter. That central, global treaty created after World War II prohibits the use of "force" by states against each other, and it affirms that states have a right of self-defense

[1] This testimony draws heavily on two previous articles: Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law,* Vol. 36 (2011) (available at *http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1403&context=yjil);* and Matthew C. Waxman, "Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions," *International Law Studies,* Vol. 89 (2013) (available at *http://stockton.usnwc.edu/ils/vol89/iss1/19/*).

against "armed attacks."[2] Historically, those provisions had generally been interpreted to apply to acts of physical violence. Questions arise today, though, as to how these provisions should be interpreted to account for the grave harms that can be inflicted through hacking and malicious code, rather than bombs and bullets.

A more legally precise way to frame the "act of war" question, then, is whether a cyber-attack could violate the UN Charter's prohibitions of force or could amount to an armed attack.[3] Even if a cyber-attack does not rise to those thresholds—take, for example, a hack of government systems that results in the theft of large amounts of sensitive data—the United States would still have a broad menu of options for responding to them. And even cyber-attacks that do not amount to force or armed attack may nevertheless violate other international law rules, some of which I discuss below.[4] However, a cyber-attack that does cross the force or armed attack threshold would trigger legally an even wider set of responsive options, which notably could include military force or cyber-actions that would themselves otherwise constitute prohibited force.

Similar questions arise in interpreting mutual defense treaties, such as the North Atlantic Treaty, to account for cyber-threats. Those commitments include collective responses to "attacks," which historically meant kinetic military attacks but might be invoked in response to attacks carried out in cyberspace.[5]

In recent years the United States government has definitively taken the public position that *some* cyber-attacks, even though carried out through digital means rather than kinetic violence, *could* cross the UN Charter's legal thresholds of "force" or "armed attack."[6] In taking that position, it has said that these determinations, in a given case, should consider many factors including the nature and magnitude of injury to people and the damage to property. Other relevant factors include the context in which the event occurs, who perpetrated it (or is believed to have perpetrated it) and with what intent, and the specific target or location of the attack. At least for cases of cyber-attacks that directly cause the sort of injury or damage normally caused by, for example, a bomb or missile, the U.S. Government has declared it appropriate to treat them legally as one would an act of kinetic violence.

---

[2] Most international lawyers agree that the right of self-defense includes right to use force in anticipatory self-defense to prevent an imminent attack, and this should be true in cyber as well, though determining the "imminence" of an attack is likely to be especially challenging.

[3] With regard to conventional military force, the United States has in the past taken the position that there is no gap between a use of "force" and an "armed attack." Many international lawyers disagree, however, and treat armed attack as a higher threshold. I have noted in the past that the application of these rules to cyber-attacks may require some rethinking of this issue. Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law,* Vol. 36 (2011), pp. 438–440.

[4] Some cyber-attacks that do not fall within these categories may, for example, still violate other international legal principles (such as the principle of "sovereignty," discussed below); specific provisions of other bodies of international law, such as space law; or a state's domestic law. As a general matter, states may respond to violations of international law that do not constitute an armed attack with "countermeasures." Countermeasures are defensive actions that would otherwise be illegal but are intended to bring a violator into compliance with international law. And even unfriendly actions that are within the bounds of international law, such as spying, may be addressed with "retorsion," or unfriendly but legal acts. Examples of retorsion would be expelling diplomats or economic sanctions in response to a hack. While I do not endorse all of its interpretations, an important survey of many of these issues is contained the recently-published *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017).

[5] NATO has declared collectively that its defense commitments extend to cyberspace, though questions of attack thresholds remain. See NATO, "Cyber Defence" (last updated Feb. 17, 2017), available at *http://www.nato.int/cps/en/natohq/topics_*78170.htm.

[6] This general position has been declared in a number of statements and official documents, including: Department of Defense Law of War Manual (Dec. 2016 edition); Paper submitted by the United States to the 2014–15 UN Group of Governmental Experts (Oct. 2014); Harold Hongju Koh, Legal Adviser, Department of State, International Law in Cyberspace: Remarks as Prepared for Delivery to the USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012).

That position has developed over time and across presidential administrations, though it remains contested and leaves open many questions. See Jack Goldsmith, "How Cyber Changes the Laws of War," *European Journal of International Law,* vol. 24 (2013), pp. 133–135. In testifying before the Senate Committee considering his 2010 nomination to head the new Pentagon Cyber Command, Lieutenant General Keith Alexander explained that "[t]here is no international consensus on a precise definition of a use of force, in or out of cyberspace." He went on to suggest, however, that "[i]f the President determines a cyber event does meet the threshold of a use of force/armed attack, he may determine that the activity is of such scope, duration, or intensity that it warrants exercising our right to self-defense and/or the initiation of hostilities as an appropriate response." Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command: Before the Senate Armed Services Committee (Apr. 15, 2010). A 1999 Defense Department *Assessment of International Legal Issues in Information Operations* that, taking account of their consequences, some cyber-attacks could constitute armed attacks giving rise to the right of military self-defense.

In explaining publicly this position, the United States usually provides only quite extreme scenarios, such as inducing a nuclear meltdown or causing aircraft to crash by interfering with control systems.

This approach to applying by analogy well-established international legal rules to new technologies is not the only reasonable interpretation, but it is generally sensible and can accommodate a strong cyber strategy. It is likely better than alternatives such as declaring the UN Charter rules irrelevant to cyber or trying to negotiate new international legal rules from scratch.

However, the U.S. Government's approach to date in interpreting the UN Charter for cyber-attacks, at least as explained publicly, may seem unsatisfactory to policymakers and planners. It leaves a lot of gray areas (though even in the more familiar world of physical armed force there are many legal gray areas). It is difficult to draw clear legal lines in advance when the formula calls for weighing many factors. And it leaves open how to treat legally some cyber-attacks that do not directly and immediately cause physical injuries or destruction but that nevertheless cause massive harm—take, for instance, a major outage of banking and financial services—or that weaken our defense capability—such as disrupting the functionality of military early warning systems.

In terms of policy, it may therefore be useful to draw sharper "red lines" than the United States has done to date—though because of ambiguities it would be difficult to use international legal boundaries alone as the basis for clear and general line-drawing. The United States has been pushing for, and should push for, certain norms of expected behavior in cyberspace (which may not be formally required), and similarly it should continue to discuss or negotiate with rivals some specific mutual restraints on cyber-attacks on particular types of targets, along with confidence-building measures.

In terms of international law, however, I do not expect that precise answers to these questions about "force" and "armed attack" will, or can, all get worked out quickly. The scenarios for cyber-attacks are very diverse and the processes by which international law develops—much of it through the actions and arguments, counter-actions and counter-arguments of states—are slow. [7]

Although the "act of war" or, more precisely, "armed attack" question usually attracts more attention, I want to raise for your consideration another relevant international law issue: the meaning of state "sovereignty" in the cyber context. [8] The United States cares deeply about preserving its own sovereignty. I would emphasize also, though, that the meaning of that concept in the cyber context—or how the U.S. Government interprets the principle of sovereignty as it applies to digital information and infrastructure—could have significant impact on the offensive and defensive operational options available to the United States. [9]

"Sovereignty" is a well-established principle of international law. In general, it protects each state's authority and independence within its own territory (and a closely related concept in international law is the principle of "non-intervention). [10] But sovereignty is not absolute and its precise meaning is fuzzy—even in physical space, let alone cyberspace. Questions could arise as to whether cyber-activities, including U.S. offensive cyber-actions or defensive cyber-measures, that occur in or transit third-countries without their consent might violate their sovereignty. Because of the global interconnectedness of digital systems, including the fact that

---

[7] As I have previously written:

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

Matthew C. Waxman, "Self-Defensive Force Against Cyber Attacks: Legal, Strategic and Political Dimensions," *International Law Studies,* Vol. 89 (2013), p. 121.

[8] Some of these issues are discussed in Brian J. Egan, Legal Adviser, Department of State, Remarks on International Law and Stability in Cyberspace, Berkeley Law School (Nov. 10, 2016).

[9] Very similar issues arise with respect to the international legal principle of "neutrality" during armed conflicts.

[10] For a discussion of these principles and some possible interpretations (among many) for cyber-operations, see the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017), pp. 11–27, 312–325.

much data is stored abroad and constantly moving across territorial borders, the answer to such questions could have far-reaching implications for cyber-operations.

I am mindful, as a policy matter, that we have a strong interest in limiting infiltration and manipulation of our own digital systems. However, it is my view that there is not enough evidence of consistent and general practice among states, or a sense of binding legal obligation among states, to conclude that the principle of sovereignty would prohibit cyber-operations just because, for example, some cyber-activities take place within another state, or even have some effects on its cyber-infrastructure, without consent. It may usually be wise to seek that consent from states that "host" digital systems that might be affected or used in cyber-operations, but I am skeptical of legal interpretations of sovereignty that impose extremely strict requirements to obtain it, especially when the effects are minimal.

This is not the setting to discuss operational issues in detail. I expect, though, that such questions about how sovereignty principles apply to cyber-operations, like questions "force" and "armed attack" thresholds, will remain the focus of intense discussion within the U.S. Government and with allies and partners abroad.

* * *

I will conclude by reiterating that existing international law, although not yet settled, is adequate to support a strong cyber-defense strategy, including a powerful deterrent. The answers to many international law questions, such as those I have discussed, depend on specific, case-by-case facts, and are likely to be highly contested for a long time to come. This means that the United States should continue to exercise leadership in advancing interpretations that support its strategic interests, including its own operational needs, bearing in mind that we also seek rules that will effectively constrain the behaviors of others.

Chairman MCCAIN. Thank you. Mr. Waxman, frankly, you raise more questions than answers. For example, if an enemy or an adversary is capable of changing the outcome of an election, that's a blow at the fundamentals of that country's ability to govern, right?

Mr. WAXMAN. Senator, I would call that——

Chairman MCCAIN. If you destroy the election system of a democracy, if you destroy it, then you have basically dealt an incredible blow to that country which is probably far more severe than shutting down an electrical grid.

Mr. WAXMAN. So, Senator, I would certainly call that a very hostile act that demands a strong response. It's certainly a threat to our democracy. Legally, though, I would not regard that as an armed attack that would justify a military response.

Chairman MCCAIN. I wouldn't call it an armed attack, but I would call it an attack that has more severe effects than possibly shutting down an electrical grid.

Mr. WAXMAN. That's correct, Senator. I think there are certain categories of activity that can have tremendous effects on states' core interests. At least traditionally, at least traditionally, international law has recognized only certain categories as justifying armed force in response.

Chairman MCCAIN. Well, I thank you, but this is really—you raise several fundamental questions that have to be resolved by the Congress and the American people.

What is an attack? If so, what response is proportionate? Should we always play defense? Should we, if we see an attack coming, should we attack first? Obviously, when we get into some of these issues concerning how we monitor possible acts of terrorism, we have this collision between the right to privacy and, of course, the public interest. But I'm sure this will be a discussion that we'll need to have with a bunch of the other lawyers on this committee.

So, as I understand it, General Alexander and Dr. Fields and Dr. Miller, we have four agencies that are responsible against cyber attacks, the FBI [Federal Bureau of Investigation], Homeland Security, Intelligence, and Department of Defense. They're the ones that are in the lead for defending the Homeland, military computer networks, employing military cyber capabilities.

It seems to me that there seem to be four different islands here. General Alexander, with your background, first of all, do you agree that the status quo isn't working? Second of all, what's the answer? What is the solution to what is clearly, it seems to me, a stovepiped scenario? We know that stovepipes don't work very well.

General ALEXANDER. Chairman McCain, I agree, it's not working. There are four stovepipes, and it doesn't make sense. If we were running this like a business, we'd put them together.

The issue now gets to both the issue that you and Ranking Member Reed brought up. We now have all these committees in Congress looking at all these, and it's messed up.

So the answer lies in a couple of areas, and I would recommend a discussion with former Secretary Gates because he and I had this, and I'll give you the gist of what we talked about, which was bring it together. We were looking at how you'd bring together at least Homeland Security, the law enforcement, and you already had the intel community and Defense Department together under one framework. I think that's where we need to go.

Before we do that, I would highly recommend that we get those four groups together and practice. Do a couple of exercises with Congress and with the Government, and potentially with industry, and show how this would and should work. I think we've got to lay that out like we do with any other operation. We haven't done that.

So what you have is people acting independently. With those schemes, we will never defend this country. More importantly, when industry looks at our government, they are, quite frankly, dismayed. We are all over the map, and no one can answer who is responsible. So you have to bring it together.

Chairman MCCAIN. Are you sure industry is that interested in cooperating?

General ALEXANDER. Absolutely. My experience—especially those who own critical infrastructure understand that they cannot defend that without government support. Working together, they see an opportunity.

Chairman MCCAIN. Dr. Fields?

Dr. FIELDS. The situation is a little more complicated because if you want to look at both defense and deterrence, you have to bring in other organs of the executive branch, like Treasury, a very effective part in this respect.

I don't see duplication of effort; I see gaps in effort, because we don't have an orchestra conductor to ensure that we don't have those gaps. Finding that orchestra conductor is not something that is easy. When we talked about it in the board we said, well, maybe the National Security Council, the National Security Advisor can play the role. We haven't had complete comfort with that as a solution.

Is that a fair statement, Jim?

Dr. MILLER. That's very fair.

Dr. FIELDS. So it is an unsolved problem. It's an unsolved problem because I actually think we do need a campaign strategy to make this a continuous process. This is not inflation exercises. The exercises are in service of high performance in executing the campaign.

Chairman MCCAIN. We should start with a policy.

Dr. FIELDS. We need a policy, and we need a strategy to execute consistent with that policy, and we need a—again, I'm going to use the term "orchestra conductor"—a more elegant term can no doubt be found—in order to make sure the gaps are filled. That, to me, is a much larger issue than some other issues in terms of is intelligence collecting the right stuff at the right time, do we have an adequate number of cyber offense folks, so on and so forth. There's a long list of execution issues. But unless we have the policy and the orchestra conductor and the strategy, we will never go where you want to go.

Chairman MCCAIN. Well, maybe for the record you can give us, all three of you, and you also, Mr. Waxman, who that conductor should be, who should be the members of the orchestra, and how legislatively we should act in order to make all that possible.

Dr. Miller, real quick.

Dr. MILLER. Thank you, Chairman. I agree with your premise, and I agree with both General Alexander and Dr. Fields regarding the nature of the solution. I'm not convinced that a massive reorganization is appropriate, certainly at this point in time, and I'd be looking toward an integrating body.

One option I believe should be considered is to build out from the so-called CTIIC, the Cyber Threat Intelligence Integration Center, which currently has an intelligence integration mission, and look to build at least toward a national counter-terrorism center model, if not towards a joint interagency task force model. If you had a so-called JIATF [Joint Interagency Task Force], it could have a civilian at the head, a military deputy, it could have different structures. But that would then bring a core team together that would be responsible for executing strategy following the policy, but to develop specific options in advance to conduct the planning and to be prepared to orchestrate responses of the nation in support of that strategy and policy.

Chairman MCCAIN. Thank you.

Senator Reed?

Senator REED. Well, thank you very much, Mr. Chairman.

Thank you, General, for your testimony. My sense from the testimony and your very astute comments is there is an interactive arrangement between strategy and exercises. You have to have a strategy to sort of get the exercise, but the exercise shows you how good or bad your strategy is.

One of the things I share with General Alexander's concern is we're not really exercising with the commercial world and the governmental world. We do it ad hoc. We have overlaps in logistics, but we have to know what some commercial companies can do, but then we have huge gulfs. Again, just quickly, your comments about how to act, because I think in terms of getting something done quickly, testing even a bad strategy or even an incoherent strategy

but just going out to see where the holes are is better than, frankly, theorizing.

So, General Alexander, your comments. Then, Dr. Fields, I have a couple of other questions.

General ALEXANDER. Yes. So, Senator, I believe that the strategy we should put in place is the government is responsible for defending the nation, and how are we going to do it, and that covers the full spectrum, whether it is our electoral system or the power grid or government; how do we do it?

Today, we take the approach that it's not doable. But let's put down a strategy that shows how we could do it, and then test that in this exercise program. That's what I think we should do. Then we'll get the organizational structure that supports it.

Senator REED. Again, we're getting to the point of if it's voluntary, some people might come and some people might not. To be effective, it's going to have to be comprehensive, and there's going to have to be a certain inducement, either an incentive or a disincentive.

Dr. Fields, your comments quickly.

Dr. FIELDS. What he said is just right. Strategy creation, exercise. Exercises go hand in hand, writing a strategy. Exercises without a strategy won't be good enough. I would add to that that we want an exercise program which consists of do an exercise, fix what's wrong, do an exercise, fix what's wrong. Too often it's open loop and not closed loop. But in any case, we're not doing it. The sooner we do it, the better.

Senator REED. Dr. Miller, do you have a comment?

Dr. MILLER. Senator Reed, I agree with General Alexander and Dr. Fields, and I would add two points. First is the task force recommendations on campaign, finding and developing an effective tool kit of potential responses, a so-called playbook of potential responses. That would be an important mechanism for getting below the level of strategy to planning, and to get to actual responses, as well as to prioritize where additional investments should be made in resilience.

Second, the type of systematic approach to exercises would also serve to demonstrate our resilience and to show gaps. But over time we'd demonstrate our resilience and begin to show the nation's willingness to respond, as well, to attacks.

Senator REED. Mr. Waxman, sort of a variation on that, because you've been talking in the context of international law, and these aspects can be incorporated also into exercises as to what do we have to stop or where do we have to refine the law, and use that as the basis. Is that accurate?

Mr. WAXMAN. That is accurate. I would echo the points that were just made and say this is an area where because of some ambiguities and gray areas of unsettled law, it's very important that lawyers be working hand in hand with the policymakers, the strategists, and the operators. This is not an area where you want to say lawyers, you go off into a room, figure it out, and then come back and tell us where the limits are.

The fact that there is some unsettled gray area in the law here, on the one hand, makes it difficult to know where the boundaries are, but it's also an opportunity if we think about this strategically.

We want the lawyers to be consulting with the policymakers on where they want to go and asking questions together, like what does a particular interpretation get us that we wouldn't otherwise be able to do; how might this limit us in other areas, let's say if we're engaging in offensive cyber operations; would this open the door to unintended consequences. So I think they need to be linked up.

Senator REED. Just a final question. I have a couple of seconds left.

Dr. Fields, you talked about deterrence, and one of the things that impressed me was that nowadays it's more of a psychological dimension than a physical destruction dimension, which leads to the target at the focus. You're really talking about individuals in the case of hypothetically between Russia and the United States, and conversely in terms of Russia and the United States from their direction, our president. Is that a fair estimate of where the new deterrence is headed?

Dr. FIELDS. The principle actually is quite old. In fact, it may be as old as mankind. You change the behavior of people, and that's what we're trying to do with deterrence, unless you decide something different, something we want.

Senator REED. [Presiding] On behalf of Chairman McCain, I recognize Senator Inhofe.

Senator INHOFE. Thank you. First of all, let me say to you, General Alexander, that it was back in 2001 that we talked about involving the university. The University of Tulsa has become quite a leader in this area. Have you had a chance to see some of the progress since you left this job?

General ALEXANDER. Yes. The last I saw, Senator, was what they were doing in industrial control systems. I think that's really good, and I think the capabilities and the students they provide back to the government is great. So I do think pushing with universities education, just as you brought up, is something that we have to do.

Senator INHOFE. Okay. The Chairman talked about the stovepipes. I want to go back and just repeat a couple of things here. The FBI has involvement in this thing, the Homeland Security, the Intelligence Committee, Department of Defense, and it's kind of in this chart all of you have seen. It's a little bit convoluted for those of us who are not as familiar with it as you folks are.

Do each of you agree that the current structure should require some fundamental change?

Dr. MILLER. Senator, I do.

Dr. FIELDS. I echo Jim's comments of a moment ago, namely reorganizing. Rewiring is not the solution; too disruptive. A fundamental change in how it works, absolutely.

General ALEXANDER. I have the chart, and I'll tell you that first, when we talk to the different agencies, they don't understand their roles and responsibilities. So when you ask them who is defending what, you get a different response. So even though this is the federal cyber security ops team, and this was put out by the White House to the commission, when we asked the individuals, they couldn't do it.

The second part that you asked is, yes, I do think, Senator, that it needs to be brought together. That's the strategy we should put

in place, how do we defend this country, and then let's walk through it, with the exercising continually evolving.

Senator INHOFE. Yes, but the reason I—last week Senator Rounds and I were in Israel, and we were talking to the head of Israel's national cyber directorate, Dr. Evatar Mitana. He said Israel has been one of the first countries to prepare for cyber security challenges using three primary processes: providing education and information on all cyber-related issues through business and industry leaders; establishing the Israeli National Cyber Authority; and pursuing the development of cyber technology throughout the country, including academic and educational institutions.

He also said during the meeting that Israel has unified all cyber operations under one doctrine, one strategy, and a single point of accountability.

I would ask, are there some lessons we could learn? Generally, we're pretty turf oriented in this country. But do his comments make any sense to you as to how they're doing it?

Dr. MILLER. Senator, your comments make a lot of sense. A common approach to engaging industry with information and a systematic effort to do that would be very valuable. I second General Alexander's earlier comments that in my experience sometimes industry is unsure with whom to engage, and the people on the government side are sometimes unsure who has that responsibility as well.

Then fundamentally as you look at going from not just strategy but to the ability to implement strategy, having a single point of accountability and responsibility below the level of the national security advisor or a deputy security advisor who ought to be focused on policy and strategy, that does make a lot of sense to me, and I think that's why the task force makes sense as a model to look at.

Senator INHOFE. I agree, and I appreciate that.

General Alexander, they told us that you are going to be speaking over there in June. You might get with them and go over this. There are always other ideas out there. Does that sound like a pretty good idea?

General ALEXANDER. Will do, Senator.

Senator INHOFE. Okay. One thing, one issue, and you brought this up, Dr. Miller, in your statement you said, "the declaratory policy that makes clear the United States will respond to all cyber attacks. The question will not be whether but how." Of course, you brought up something, Dr. Fields. In your eighth point you said, "Credibility is a necessary enabler of deterrence. If a leader we want to deter does not believe we will act, it is difficult to deter. Announcing red lines and then overlooking offenses is not constructive."

I think that that has happened. How do you reestablish credibility, assuming that some of it has been lost?

Dr. FIELDS. You reestablish credibility not by making a declaration alone but by acting. We have so many cyber intrusions going on every day that there's plenty of opportunity to act.

Senator INHOFE. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN. [Presiding] Senator Shaheen?

Senator SHAHEEN. Thank you, Mr. Chairman.

Thank you gentlemen for being here today.

I would like to pick up on Senator McCain's point about the Russian hacking into our electoral system because, Mr. Waxman, I do believe that that's a strategy that Russia is using, just as they're using military conflict, propaganda to undermine Western democracy. So I think we should think about whether it's an act of war or not.

I was in Poland with Senator Durbin last week, and one of the things that we heard from some of the civil society leaders in Poland was they were asking about the hacking of our electoral system, and they said if the United States isn't going to take any action in response to that Russian intrusion against your elections, then how can we think that the United States is going to take any action to protect us against Russia?

So, Drs. Field and Miller, given your credibility is a necessary enabler of deterrence, and if a leader we want to deter does not believe we will act, then it's difficult to deter, what kind of message does it send to Vladimir Putin and to the rest of the world if we don't take action in response to Russian hacking in our elections? I'm happy to have anybody answer that, or General Alexander.

Dr. FIELDS. I don't feel qualified to observe whether or not hacking into our election is an act of war or isn't an act of war.

Senator SHAHEEN. I'm not asking you to determine on act of war. I'm asking what message it sends to others who are looking at the United States' response to that hacking.

Dr. FIELDS. I think the question that I'm worried about is what do we want to do so that it doesn't happen in 2018 and doesn't happen in 2020. Taking no action guarantees escalation. Taking action has the possibility of escalation but also the possibility of deterrence. There are many possible actions we can take, not for this hearing, unclassified, but we have to do it.

Senator SHAHEEN. General Alexander?

General ALEXANDER. Senator, I think we have to do two things. One, I do think we have to push back overtly so that the rest of the world knows that, but we also need to fix our defense. It's wide open, and what happened, and what's been happening, people can get in and take what they want. Without any defensive architecture or framework, that's where we are. So we ought to do both. We ought to push back, but we also ought to fix our defense, come up with a comprehensive strategy. We can defend this country in cyberspace. We're not doing it, and that's what I think we need to do.

Senator SHAHEEN. Well, I certainly agree with that. That makes sense.

To your point about cooperating with the private sector, the Department of Defense has issued regulations that require all DOD contractors, including small businesses, to comply with a series of cyber security requirements by December 31st of this year. As part of this rulemaking process, the Small Business Administration—I sit on the Small Business Committee, so that's why this has come to my attention—their Office of Advocacy has claimed that DOD underestimated the number of small businesses that are going to be affected by the rule, the costs of the rule, and the ability of

small businesses to comply. In the final rule issued last October, DOD claimed it was not feasible to implement recommendations from the Office of Advocacy to provide some financial help to small business and some guidance, and they admitted that the cost of complying with the rule was unknown.

Now, this week I had a small business contractor from New Hampshire in my office who was very concerned about how to comply with these requirements, and not even having information about what they needed to do to comply.

So I guess my question for you, General Alexander, is should DOD be doing more to work with small businesses, and do you have any recommendations if the commission looked at this, and does it have any recommendations on how to help small businesses comply?

General ALEXANDER. So there are actually two sets of issues that you bring up. First, it is really difficult to comply with these types of standards. One is the international standard 27,001, one is the NIST [National Institute of Standards and Technology] framework. As you look at it, how do companies certify that they've met all of those? That's a year-long process. It's very expensive, and you need a lot of people to do it. So a small business that has five people, it's going to be difficult.

So I think we have to set up realistic expectations. How do they do that, or could they sub to a contractor who has that authority? The answer is I think you can get there. We are actually going through that in my company, so I can tell you how hard it is. We're doing it, and we have some people with perhaps some security background. So when we look at it, it's very difficult.

The second part, think about all the industrial control systems out there. The standards on those are even worse. If you look at the threats that hit the Eastern seaboard last fall, it was caused by, in large part, by printers and by cameras and other things that had been coopted to help in the distributed service attacks. There is no way that we can today ensure that those are protected. So the IT [Information Technology] portion of the commission, what we've laid out there is you need to come up with some way of measuring how companies do that, first in the United States and then globally.

Senator SHAHEEN. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN. Thank you.

Senator Fischer?

Senator FISCHER. Thank you, Mr. Chairman.

Dr. Miller and Dr. Fields, the Defense Science Board recently released a final report on cyber deterrence and included a recommendation that the commander of CYBERCOM should develop scalable and strategic offensive cyber capabilities in order to deter cyber attacks against our critical infrastructure here in this country. Can you elaborate on this and what types of capabilities the DSB believes are needed, and tell us what the basis was for that recommendation?

Dr. MILLER. Senator, the basis for the recommendation was that although the United States should have the available option of not just cyber but other responses, whether diplomatic, economic and

so forth, that one of the most credible potential responses in offensive cyber in use against us is to use offensive cyber back against the state that undertook the attack. Following what Dr. Fields talked about, what we want to do in developing that portfolio of options to go against Russia or China or North Korea or Iran in particular is to look at the leadership values and to look across a range of potential targets that would hold at risk what they value. Then the value of having this, the campaign funding that we talked about, is to have a sense of what level of response and what specific types of targets might be most appropriate for a given scenario, and there's a risk of both doing too little, responding too weakly, and there's a risk of responding too strongly in the sense that in some instances you may want to reserve something to deter additional attacks.

So that's the fundamental structure of it, and as you look at those strategic options, the final point is to differentiate between those cyber actions by the military that are intended to have tactical or operational level effects on the battlefield and those that are intended to have psychological effects on the leadership of our potential adversaries.

Senator FISCHER. As you said in your opening, you're weighing the cost and the benefit, the increase and the decrease, on each of these; correct?

Dr. MILLER. Yes, ma'am. In fact, when we look at the offense, we're looking to increase the cost of a potential adversary using cyber attack or these costly cyber intrusions against us and our allies and partners.

Senator FISCHER. Another recommendation in the final report focused on acquisition of these offensive cyber capabilities. Specifically, it called for improved and accelerated acquisition authorities for CYBERCOM and also the establishment of a special organization for rapid acquisition.

In the fiscal year 2016 [NDAA National Defense Authorization Act], the Emerging Threats and Capabilities Subcommittee, which I chaired at that time with Senator Nelson, included language that provided the commander of CYBERCOM some acquisition authority. In the fiscal year 2017 bill, it greatly expanded the commander's role in the requirement to process. I know some of the changes are still waiting to be implemented, but can you talk about how this dovetails with what the DSB was thinking, and are there other areas where further congressional action would be helpful?

Dr. MILLER. I'm glad to respond first and then turn it to my colleagues. In my view, it does dovetail very nicely with the prior congressional action. The recommendation we had was to establish a small team that had not just support but direct access to the senior leadership that would then look at how the efforts to date are going with respect to CYBERCOM acquisition authorities, to look at something like a rapid acquisition team. It could be embedded within CYBERCOM. It could be embedded beside it, in principle. What other steps should be taken, because although rapid acquisition is important in general, if you look at cyber tools and moving potential targets that we face, it is particularly important to be able to do that more quickly than we have to date.

Dr. FIELDS. I want to be sure that the committee is calibrated properly on the speed that Jim is talking about. We're used to, in acquisitions, a system that responds in years. For this we need days and weeks, maybe less. It's a rapid-fire exchange. If we can't respond, we lose.

Senator FISCHER. Thank you, sir.

Thank you, Mr. Chairman.

Chairman MCCAIN. Thank you.

Senator Kaine?

Senator KAINE. Thank you, Mr. Chairman.

Thank you to the witnesses.

General Alexander, in your testimony you have a quote: "We must fundamentally rethink our nation's architecture for cyber defense," and all of the testimony today is a tribute to that. I want to switch gears to a closely related topic, which is information warfare. That's often closely connected with cyber attacks. So much of cyber attacks is to suck out personal information, and then with that personal information you can target false information to people, and it's part of a propaganda campaign.

Last week, Russia's defense minister appeared in their parliament and bragged about the Russian military's new information warfare and propaganda efforts. We had testimony here from Director Clapper in January, and he said, quote, "We need a U.S. information agency on steroids to fight this information war a lot more aggressively than we're doing right now, one that deals with the totality of the information in all forms, to include social media." ISIL [Islamic State of Iraq and the Levant] is also using social media platforms to do this kind of thing.

Do you agree with Director Clapper's assessment, and what role do you think the public and private sector should play in an effort to counter information warfare connected to these cyber attacks?

General ALEXANDER. Senator, thanks. That's a great question. I'm not fully aware of all of Director Clapper's comments, but I do believe that we have to have some way of looking at how countries are pushing at us using information warfare and what we do on that. It gets to some really tough issues that have to be integrated across the entire government.

As a consequence, some of the comments that we made earlier about an organized and central framework for this is what we're going to need to do. One of the questions that you put out to all of us was is there an organizational structure that needs to occur, and I think that's part of what needs to be tested in a strategy that we put out there.

I think the government needs to say here's how we're going to defend this country from these types of attacks, whether it's information warfare or destroying data or stealing data, and we ought to then go through and see what the roles and responsibilities of each organization are. If it's a nation-state and there is a possibility or probability that it will lead to war, then it's my belief it should be the Defense Department. If it's a law enforcement, then FBI/Justice. When I dealt with Director Mueller, we had a great partnership. We worked together eight years, and we had a great division of effort there. There were no seams between us.

We can get there and do this, but there's no architecture today, Senator, and that's what I think we need to do.

Senator KAINE. Other thoughts?

Dr. MILLER. Senator, I'd like to add that from my perspective—this is not reflecting the Defense Science Board—from my perspective, because we are in a competition between models of government as well with respect to Russia and China, it seems pretty obvious to us and our allies and partners and most of the globe which is the preferred model. But we need to build on our strengths, and that includes a free press.

So I would suggest that a fundamental goal should be to knock down fake news. As we think about that, we think largely of rhetorical steps, but cyber is a tool to knock down fake news and to take down fake websites and so forth. Having a set of rules of engagement and policies associated with that I believe could be valuable as well. I just want to emphasize the point that the last thing that any of us I know would want is something that would be portrayed or have any sniff of the type of propaganda that we're seeing from some of these other actors.

Senator KAINE. Yes, we want to counter it but counter it in accord with our values, not contrary to our values.

Dr. FIELDS. You were correct in noting that information ops, influence ops of the sort you're talking about, go beyond cyber and not only include cyber. Some examples: a foreign power buying a television station so it can make its point of view known because television is so influential; making campaign contributions through cutouts to particular political candidates. It's widespread.

Last summer we spent a great deal of time on this, and we had 80 people working 9 months to come up with a set of actionable recommendations of how to both conduct and counter such operations. It starts with good intelligence collections, and know they're happening, and it goes beyond that into both defense and deterrence.

So again, this is something that we can do. We just aren't doing it.

Senator KAINE. Great. Let me just ask one other question quickly, workforce. The DOD used to have a scholarship for service program for cyber students. It helped about 600 students learn cyber skills and then work at the DOD in cyber fields. That program within DOD was scrapped in 2013 during a period of the sequester and budgetary confusion.

There is a similar program, a kind of ROTC [Reserve Officers' Training Corps] type program that is done through the National Science Foundation called Cyber Corps. But are programs like this necessary to try to bring in the talent that we need to ultimately fill the structure that we hope we might create that would be effective?

General ALEXANDER. I believe so, and I would take one step further. I think we should really push science and technology and engineering and math for the ROTC and the military academies as a strong, fundamental thing that students should understand, because as future leaders they're going to be expected to help guide their people to this, and if they don't understand it, they're not going to be able to do that.

Dr. FIELDS. I would just add that there isn't a comprehensive program of the sort you're talking about and there should be. There are activities. DARPA [Defense Advanced Research Projects Agency] was very, very active in trying to engage young people, holding contests, and it's really very effective, if not comprehensive.

Senator KAINE. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN. Thank you.

Senator Rounds?

Senator ROUNDS. Thank you, Mr. Chairman.

Mr. Waxman, I find it fascinating the discussion on sovereignty and the challenges that that would have for our country when we're talking about other players, whether they be first-tier competitors or non-country actors, non-national actors. They don't seem to have much concern about whether or not they move through the cyber world in the sovereignty area of other countries, or at least those areas that may very well come through lines that are in other countries.

TALLINN 2.0—and you and I have discussed earlier that TALLINN 2.0 has not been released, and the discussion there has to do with sovereignty, and some of our allies may very well have a different point of view of what sovereignty should be considered with regard to cyber security.

Could you share with us a little bit the challenges that we have if we don't come up with an appropriate determination for what sovereignty really means and the impact it has on our ability to come back in and respond to an attack?

Mr. WAXMAN. Sure, Senator. I do worry about some overly-restrictive interpretations of sovereignty. As I said in my opening statement, I'm concerned that some interpretations of sovereignty would go too far in limiting both our offensive cyber as well as our defensive cyber operations, especially if they involve cyber activities with relatively small effects on unconsenting third countries.

As you said, recently published is a book, an effort called TALLINN 2.0. This was something that was conducted under the auspices of NATO's Center of Excellence for cyber issues, and it's an impressive and very important product for surveying the many international law issues that come up. I don't agree with all of its conclusions, though, and in particular I worry that it's an example of overly-restrictive interpretations of sovereignty that could needlessly and perhaps dangerously restrict our operational flexibility.

Senator ROUNDS. Thank you.

Any other thoughts or comments on that particular issue among the rest of the members?

Dr. MILLER. I don't want to give you a legal opinion because I'm not a lawyer, but I will say that some policy steps can be taken that can reduce that. For example, if we work with our allies and partners to have reciprocal arrangements where if we see something on their networks that's a threat we will take care of it, understanding that the presumption would be that there is no or minimal side effects associated with it, this could allow faster action, at least within that federation of allies and partners. I think there are a number of other steps that we should be looking at, and it reinforces Mr. Waxman's earlier point that the lawyers and pol-

icy people have to work closely together, and to do so in real time, the real world, and working through real problems.

Senator ROUNDS. Thank you.

Dr. FIELDS. Just to add that the Internet knows no bounds. If there is a communication, one communication might go through many countries, and we might not even know what countries it goes through. That's an issue, and also that our adversaries are mindful of our concerns on this matter and have the opportunity to locate their facilities in places where we don't want to go because of our concerns with sovereignty. That's using the cracks, the seams that we attend to is not really helpful for us. Intentionally or not, that's what they're doing, and in most cases intentionally.

General ALEXANDER. Senator, I would take one step further and say, for example, ISIS [Islamic State in Iraq and Syria] and other terrorism on the network, we shouldn't allow it, and we should work with our allies. If they have anything on that network, we should all work to take it down and identify where it is and tell those countries to take it down.

There are things like that that are criminal in nature that we ought to all push for. The Internet isn't a free way for them to go out and recruit and train people and get funding. We ought to shut that down, and we ought to look at what are the other core values that we share with countries in this area that we could do. You've got those on child pornography and other areas. So we ought to just put that out there and do it.

Senator ROUNDS. The supply chain for civilian and military technology is largely shared and increasingly produced offshore, particularly in the realm of microcontroller enterprise management software. This marks the first time in history that a critical weapons system is potentially dependent on commercially produced components which are produced overseas, perhaps by one of our allies and which, if subject to tampering, could create a cyber vulnerability for one of our weapons systems.

My question is, what is your policy recommendation for securing the IT supply chain that originates in foreign countries to include our allies? One small part of it, but I think an important part of it.

Dr. FIELDS. We have a very large study with a dozen recommendations for specific things the Department can do in order to mitigate the risk. Bringing all microelectronics back on shore is not going to happen. Mitigating the risk can happen. I can't do justice to that report in minus 21 seconds, but there are really things we can do. It's not impossible. The options are available.

Senator ROUNDS. Mr. Chairman, thank you.

Chairman MCCAIN. Senator King?

Senator KING. Thank you, Mr. Chairman. I think this may be the most important hearing that we've had since I've been here, and I want to put a fine point on that. To me, the most chilling finding of the board was—and this is a direct quote—"The unfortunate reality is that for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructure." That is a powerful statement, and it seems to me that what we are observ-

ing here is a fundamental change in the nature of warfare that's occurring right before our eyes.

The historical example I think of is the Battle of Agincourt in October of 1415, when a ragtag British army of 7,000 soundly defeated a French army estimated between 20,000 and 30,000. The British lost 600. The French lost 7,000. The difference was technology, the long bow. That is what changed the course of history, and it was because the mightiest army in the world, the French, did not wake up to the change in technology represented by the long bow.

We're the mightiest military in the world right now, but for the cost of one F–35 the Russians can hire 5,000 hackers, and we are seeing this happen. What bothers me, Mr. Chairman, if there is an attack—and I don't think it's if, I think it's when—and we go home, and I go home to Maine and say, well, we couldn't really defend ourselves because we had four committees that couldn't get the jurisdiction together, I don't think anybody in Maine is going to buy that.

So we've got to get this right. If you're right, that technically we can't defend ourselves, then deterrence is the only answer. So I have several questions on that.

One is you list your eight principles of deterrence, which I think are very important. One that's not there, I think number 9 is whatever we have for deterrence has to be public. It's not deterrence unless the other side knows what's there.

Do you concur that there has to be some, maybe not all the technical things that we have, but people to be deterred have to know there's a threat they're going to be whacked with if they come against us?

Dr. FIELDS. My list is much longer, but I tried to keep it to 5 minutes. So your addition is a good one, but there are several others as well. What you say is absolutely correct.

Senator KING. Well, I think we've got to have the capacity to deter.

The other question, and this gets back to my comment about congressional jurisdiction and committees, does this need congressional action, or is this something the executive has responsibility for because of their being the Commander in Chief? Is this something that can be done within the organization of the executive branch, or is there legislation necessary? If there is, tell us what it is so we can move on it.

General Alexander?

General ALEXANDER. If I could, I think, Senator, that, one, if we go the path we're on right now, we will be behind in 10 years. But I do believe there is a solution out there where government and industry could work together and provide a much better defensible——

Senator KING. Much better, but do you think it's capable to defend entirely? I don't think that's possible technologically.

General ALEXANDER. Well, you see, I think what we should do is say how do we want to do that, and then put together a framework to do it, and test it. But right now what we've done, in my opinion, is we've said it's too hard, and I actually believe it can be done.

Now, will it be perfect in the first five years? Probably not. But I think we could set together a framework to defend this nation where industry and government work together.

Senator KING. Well, I don't think we have five years. This is the longest windup for a punch in the history of the world.

General ALEXANDER. Right, so we ought to get on with it. What we've done since 7 years ago when I went before this committee—thank you—and you guys confirmed me despite all that, at that time we talked about defending this country. Here's how I think we should do it. Put together a framework, but also have the rules of engagement so when somebody comes at us, we go back at them.

Senator KING. That gets to my point about it has to be public. People have to know what the rules are.

General ALEXANDER. That's right, exactly, and we don't have those, so we ought to create it. I think it's a combination between the administration and Congress, because there is going to have to be some reorganization that will come out of this strategy and training. But we ought to do it. We've spent—year after year we come back and have the same meeting, and we're not getting progress. We need to get this fixed.

Senator KING. I agree. Thank you.

Dr. MILLER. Chairman, can I add very quickly, Mr. Chairman? There's no question there's an important role for Congress. We're seeing some of it today, but funding, organizational change, policy issues and so on.

I want to emphasize that it's fundamentally important to improve the defense and resilience of our critical infrastructure. It was the judgment of the task force that even with substantial efforts there, we are not going to be able to prevent the most capable actors, by which I specifically mean China and Russia, from being able to——

Senator KING. That was the sentence I read.

Dr. MILLER.—get in to produce significant, if not catastrophic, effects. But we can raise the level of difficulty for them so it's more challenging for them. That will give better indicators, a better chance to interdict, as General Alexander talked about, and fundamentally so that we don't allow us to get into the same position with respect to an Iran or a North Korea or a terrorist group, which is completely untenable.

Chairman MCCAIN. But doesn't this go back to what won the Cold War? Peace through strength. If they commit one of these, a price, that they would pay for it, that it would be unacceptable. Rather than trying to devise—General Alexander said 5 years or so to construct the defenses. In the meantime, the response will be such that it will cost them a hell of a lot more than anything they might gain. Does that make any sense?

General ALEXANDER. Absolutely. What we do right now is there are no rules of engagement and there is no integrated infrastructure between industry and the government. Both of those are things that could and should be done in parallel.

Chairman MCCAIN. But as all the witnesses have said, we don't want to create another bureaucracy, right?

Senator Wicker?

Senator WICKER. Mr. Chairman, if Senator King wants to quote a few lines from the St. Crispin's Day speech, I'll yield him two minutes.

[Laughter.]

Senator KING. "Oh, ye brothers, ye band of brothers, ye precious few."

Senator WICKER. But this is a different bunch we're talking about in this day and age.

Gentlemen, in the paper from Dr. Fields and Dr. Miller, we have three cyber deterrence challenges—Russia, China, regional powers, Iran and North Korea, and then the non-state actors. I don't want to ask you to reiterate things that have already been said, but I did check with staff and I understand we haven't really had much of a talk about the non-state actors.

Senator King mentioned to defend versus deter, and particularly with regard to the non-state actors, a deterrence against them would have to look far different from a deterrence against a nation-state. So would anyone like to help us out on that?

Dr. FIELDS. To date, non-state actors haven't demonstrated the cyber power that the major state actors have demonstrated. That won't last forever, but it's the case today.

So today, a reasonable approach to non-state actors is, in fact, a defense strategy with a little bit of deterrence. At the point where we have to deal with deterrence as their power grows, their capability in cyber grows, the same principles apply but all the details would be completely different.

We have to identify them, we have to identify what they hold dear, we have to understand what the leaders hold dear, all the things we said earlier. We're not at that point yet, but inevitably we will be.

Dr. MILLER. I'll just add very briefly that as we think about non-state actors, we want to differentiate between two broad groups. One is a set of criminal activists and so on, that we would expect that would be subject to cost-benefit calculations, and if we have credible threats, to impose costs on them, that we can be successful with a deterrence strategy. It doesn't mean stopping all criminal hacking and so forth, but being able to impose costs, and that should be a fundamental part of the strategy.

As we think about terrorists groups, any groups that are willing to not just cause the loss of life but have its members lose their lives, whether through suicide bombings and so on, we really do need to focus on deterrence by denial and a defensive posture. As we think about that defensive posture, it's not just rope-a-dope. It's also the ability to preempt, as we do for other terrorist threats.

Senator WICKER. Deterrence by denial.

Dr. MILLER. By denial it means that we're looking to reduce any benefits that they would gain, and in the case of terrorists in particular, to prevent them from the ability to conduct an attack, deny them either the ability to conduct the attack through preemption or prevention, and then reduce the benefits, in a sense, and the reduction of benefits from their perspective comes by hardening our infrastructure.

Senator WICKER. Yes, sir, General Alexander.

General ALEXANDER. Senator, you bring out a good point that binds together what Senator King and the Chairman brought up, which is non-nation-state actors, we should be elevating the defense so they can't get in and cause it, cause a problem for us, and we can do that and should be building that.

On nation-state, just as the Chairman said, we go back to them and say if you do A, we're going to do B, and let them know it, and then do that. I think that's how we get through the next few years while we continue to evolve our defense. But there is a way to do this, and I think we can do both.

Senator WICKER. We haven't really sent very good signals the last few years about consequences and crossing lines.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Warren?

Senator WARREN. Thank you, Mr. Chairman.

Thank you all for being here today.

I want to follow up on this question about the distinction between cyber defense, stopping a hacker before they can do damage, and cyber deterrence, as Chairman McCain was talking about, preventing a hacker from ever making the calculation that it's worthwhile to try to attack the system in the first place.

I go back to what Chairman McCain and Senator Shaheen were talking about, the information gathered by CIA [Central Intelligence Agency], the FBI, NSA. The Director of National Intelligence recently assessed with high confidence that the Russian government conducted an influence campaign aimed at the U.S. presidential election which included both propaganda and covert cyber activity, and I think most senators would agree that is completely unacceptable in the United States.

So for 70 years the U.S. has had a policy of nuclear deterrence that has been a bedrock of our security. Given what happened last year, it seems clear that we need cyber deterrence, not just defense but deterrence as well. I know that, Dr. Miller and Dr. Fields, you've issued a report on this. We want to talk about the organization of how that would work, but I want to ask a different question, and that is substantively, what should the United States do to deter these types of attacks in the future? At least describe somewhat the range of options that are available to us for deterrence, not defense but deterrence.

Dr. Miller?

Dr. MILLER. Thank you, Senator. I'll defer coverage of some of the key elements. I'll just emphasize three of them in particular.

First, in order to avoid being reactive, you've got to do prior strategy and planning, and that includes communication to our potential adversaries that there will be a response to any cyber attack, or what we call costly cyber intrusions, supporting information operations and so on. That planning process needs to be in a campaign construct so it's not just one-off and so on, and it means that that plan is being executed every day. You're looking to influence the perception of the leadership of these countries about the viability of any such actions.

To reiterate earlier points, as we think about Russia we need to think not only about the 2018 elections here but about our allies' elections that are coming up in Europe in the coming year.

So first is a campaign planning construct.

Senator WARREN. Okay. So I'm hearing you say be sure that they know what we're going to do. I'm not sure I'm hearing what the range of options are for us to do.

Dr. MILLER. So then the range of options. For years we've said that we will not limit ourselves to cyber responses, to cyber reactions, and that's fine. Fundamentally, our recommendation for declaratory policy and for real action is that the United States Government, the President can say if we are attacked with cyber, we will respond.

So what is the range? The response is going to depend both on who is attacking and what is their purpose. One thing you want to do is deny their benefits. In the case of Russian hacking of various accounts to try to influence our election and to try to denigrate our model of governance, prevention, including in my view getting that information out earlier, would have been very helpful.

Then the specific responses would be looking at what imposes costs on President Vladimir Putin and his inner circle that would cause them to not just pause and reconsider but to not conduct this type of activity in the future. It will not have zero escalation risk, as Dr. Fields talked about before. So it includes offensive cyber, it includes more significant diplomatic and economic steps.

Senator WARREN. Dr. Fields, do you want to add something here?

Dr. FIELDS. I do, two things. Number one, we're not quite answering your question——

Senator WARREN. Yes, that's right.

Dr. FIELDS.—because we'd like to do so in closed session.

Senator WARREN. All right. Fair enough.

Dr. FIELDS. We can in closed session.

Number two is in terms of this defense/deterrence issue, which I consider we need both, the fact is that today, 2017, the techniques that the best cyber offense people can use trump the techniques that the best cyber defense people can use. That may not be true five years from now because the defense capabilities are improving, but so are offense capabilities.

Senator WARREN. But doesn't that argue, then, even more strongly for a deterrence strategy?

Dr. FIELDS. Absolutely.

Senator WARREN. Rather than relying exclusively on a defense strategy, and not confusing a defense strategy with a deterrent strategy, as I heard it discussed earlier?

Dr. FIELDS. That's why we did our study, and you'll notice that the study actually included some defense elements as well, but those would be for certain cases, for certain actors, and really at a lower level. The top level should be deterrence.

Senator WARREN. I appreciate that, and I recognize I'm over my time. It sounds like Mr. Waxman would like to add, but that's up to the Chairman.

Mr. WAXMAN. Thank you, Mr. Chairman, because this actually goes back to your question before about Russia. I was cautious in how I would classify the Russian action as a matter of international law because political interference is not an uncommon thing in international affairs.

However, the fact that I'm cautious in how I'd classify it does not mean we need to sit back and take it. There are a menu of options that ought to be part of our policy in deterring these kinds of actions, including sanctions, including engaging in our own cyber operations, diplomatic steps, intelligence operations, law enforcement operations in certain circumstances, and even taking some military steps to apply pressure, such as moving forces, conducting exercises, providing more military assistance to our allies.

Senator WARREN. All right. That's very helpful.

I just want to say on this, nuclear deterrence works in part because we all knew it was out there. When we can't describe even in the most general terms what will happen if you engage in a cyber attack against us, and indeed it's clear that we have been the victims of a cyber attack by the Russians, and we can't describe any kind of response to that, it seems to me that deterrence at that moment melts away to nothing. So I'm glad to take this into another setting to hear more about it, but there has to be some kind of response that is publicly known.

Thank you, Mr. Chairman.

Senator PETERS. Thank you, Mr. Chairman.

Thank you to our panelists for a fascinating hearing here.

In 2016 the NDAA, specifically section 1647, Congress provided funding enabling the DOD to accelerate cyber mission assurance efforts relating to major weapons systems and platforms. These cyber assessments, of course, are critical to ensuring that key DOD systems are free of adversary threats and resilient to cyber attack, particularly in contested environments. But in parallel, I do have a concern, and actually echoing the concern that Senator Rounds mentioned in his questions.

We have a limited understanding of supply chain risk in the defense industrial base. As all of you know, these risks could include counterfeit components that end up in war-fighting platforms; or worse, undetectable hardware or software modifications that are perpetrated by a very sophisticated adversary.

I know, Dr. Fields, you began to answer the question and didn't have sufficient time. I'd like to give you some time now to tell us exactly what we should be doing.

Dr. FIELDS. As I said, there's a pretty long list of things to do, and I'll give you some examples, concrete examples without naming names.

If you find something that's wrong with one of your systems, you should have a database of knowing where all of the other systems are so that you can actually stop using them and repair them. You should know where that component is in other systems. You should check in advance the supplier that's providing it to see what else they have provided. Everything I'm saying and would say if we had much more time, that's just common sense. It takes a lot of work to do it, and we're starting to do it. It would be wrong to say DOD is not starting to do it, but there's also a long way to go.

Senator PETERS. Sometimes you don't find out something is wrong with a system until it's too late.

Dr. FIELDS. That's also the case.

Senator PETERS. So how do we deal with that?

Dr. FIELDS. There are going to be such cases. In fact, we can build systems, although we don't always do so, that are more fault tolerant, because many of the things that are put into microelectronics are very similar to what happens when a mistake is just an accidental mistake, and we do work hard to design systems that compensate for accidental mistakes.

So again, we can do better. I know I'm not giving you a very complete answer because it would take another hour. But there is actually a whole action list of things to do that the Department has started to do.

Senator PETERS. I'd like to spend more time with you. So maybe offline we'll be able to spend that hour talking more in-depth about this, because I think it's a significant issue that was brought to my attention by some other suppliers that have issues, or concerns I should say, related to that.

Being proactive—this is a question really for General Alexander—do you believe that the Department's cyber protection teams have the background information necessary to assess which systems, components, software, and organizational processes may have exploitable supply chain vulnerabilities?

General ALEXANDER. I think that's going to be a continuous work in progress, Senator. I think getting the information, because these systems are changing every couple of years, the technology that's going in, especially in the IT area, that's something that they have to be on top of. You bring out a good point. The cyber protection teams have to work with the customers they're supporting, and if we look at where we put them, that may include industry as well, and parts of critical infrastructure.

That's a big set of technology area that these teams have to be up on, and so constant training. Are they there today? I doubt it. I think they're working towards that.

Senator PETERS. All right. Thank you.

The next question relates to the U.S. semiconductor industry which, as all of you know, is facing some major challenges here. In addition to confronting the fundamental technological changes that are moving the industry, there's also been a very concerted push by the Chinese to reshape that market in their favor using industrial policies that are backed by hundreds of billions of directed government funds. With semiconductor technology critical to defense systems and overall military strength, China's industrial policies I think pose some real threats for semiconductor innovation in the U.S. national security interest.

I know that we have a range of tools to deal with this, including the CFIUS [Committee on Foreign Investment in the U.S.] committee, but while the overall number of CFIUS reviews has risen steadily since 2008, the increase, as you know, is disproportionately small when compared to the ratio of completed transactions.

So, to the panel, if CFIUS is unable to slow China's advance, what are the implications for United States technological superiority, in your mind?

Dr. FIELDS. My colleagues turned to me. We've done several studies on this over the years, we being the Defense Science Board, and I'm sorry to say that we've come up with no solution that I'll call a good solution. We have solutions for some things; not for this. In

some areas we can continue to stay ahead. I'll call those areas software and some aspects of manufacturing. But this has proven to be a tough nut to crack. So I can offer you nothing that I have confidence in.

Senator PETERS. A tough nut to crack, but one that we have to crack.

Dr. FIELDS. Yes.

Senator PETERS. Thank you very much, appreciate it.

Chairman MCCAIN. Mr. Waxman, during the debate on how we would combat terrorist attacks in the United States, we got heavily into this issue as to when government should intervene, and yet we should also respect the fundamental right of Americans to privacy. Do you see that issue looming here as we try to counteract or improve our ability to address the issue of cyber?

Mr. WAXMAN. Yes, Senator, I absolutely do. I think where I've seen it certainly very present is in legislative discussions about improving information sharing between the private sector and the government. I think pretty much everybody agrees that that's critical to improving our cyber defenses, but I think the public and certainly segments of the public are very wary of sharing information with the government. Companies in some cases are leery of giving information to the government because they fear criticism on the civil liberties front.

Chairman MCCAIN. So we're really going to have to wrestle with that issue when we heed the recommendation of this committee of a much closer relationship between industry and government.

Mr. WAXMAN. Yes, Senator.

Chairman MCCAIN. It's not easy.

Mr. WAXMAN. No, Senator.

Chairman MCCAIN. But given the fact that you're a great lawyer, you're going to give us the answer. Is that right?

Mr. WAXMAN. I hope so, Senator. I also think this is one reason why issues of cyber security, surveillance, other intelligence activities are interconnected. Certainly a big issue here is improving trust that the public has in intelligence agencies, and anything that we can do to build and improve that trust will pay dividends when trying to come up with solutions on cyber security.

Chairman MCCAIN. Well, General Alexander, on your watch, you gave us a lot of confidence, and we are very glad that you are back here before the committee, and we will continue to call on you for your unique experience and knowledge.

I want to thank you, Dr. Fields and Dr. Miller. It's great to see you again.

This is going to be not the beginning but sort of the beginning of a series of hearings that this committee has to have. We understand a lot of the conventional weapons and strategic weapons. I don't think amongst this committee or amongst the American people the dimensions of this challenge are fully understood. Until we fully understand the dimensions of the challenge, then I'm not sure we're able to address it adequately from a legislative standpoint. I think we would all agree that first we have to have a policy, and then we have to have a strategy, and unfortunately we have not achieved that first wicket in this process that we're going through.

I'm especially grateful that you're here today because right now, besides funding, this is the highest priority that this committee should have, and I think if you're looking at vulnerabilities that this nation has, that that's an appropriate priority.

Senator Reed?

Senator REED. Mr. Chairman, I concur entirely. I thank you again for hosting this hearing. I think it's our mutual desire and wish that these hearings lead to prompt remedial action, and I know with the Chairman's leadership that will happen. Thank you.

Chairman MCCAIN. I thank the witnesses.

General, I promise we won't make you come here very often.

Thanks again.

[Whereupon, at 12:03 p.m., the committee was adjourned.]

CYBER POLICY, STRATEGY, AND ORGANIZATION

THURSDAY, MAY 11, 2017

U.S. SENATE,
COMMITTEE ON ARMED SERVICES,
Washington, DC.

The committee met, pursuant to notice, at 9:30 a.m. in Room SD–G50, Dirksen Senate Office Building, Senator John McCain (chairman of the committee) presiding.

Committee members present: Senators McCain, Wicker, Fischer, Cotton, Rounds, Ernst, Tillis, Perdue, Sasse, Reed, Nelson, Shaheen, Gillibrand, Blumenthal, Donnelly, Hirono, King, Warren, and Peters.

OPENING STATEMENT OF SENATOR JOHN MCCAIN, CHAIRMAN

Chairman MCCAIN. Well, good morning. The committee meets today to receive testimony on cyber policy, strategy, and organization, of which there is very little.

We are fortunate to be joined this morning by an expert panel of witnesses: General Jim Clapper, who enjoys nothing more than testifying before Congress and is making his second appearance on the Hill this week. I hope you are scheduled for a couple more next week. Anyway, General Clapper, there is a reason why you are in demand and that is because of the incredible esteem in which you are held by Members of Congress. I know that this is not your favorite activity, but I would argue that this issue deserves your input and your knowledge and background.

Jim Stavridis, who is the Dean of the Fletcher School of Law and Diplomacy at Tufts University and former Commander of U.S. European Command, in which he did an outstanding job. It is not his first appearance before this committee.

Michael Hayden, Principal at The Chertoff Group and former Director of the Central Intelligence Agency and the National Security Agency. Again, a man of great credentials.

As Admiral Rogers told this committee earlier this week—and I quote—we face a growing variety of advanced threats in cyberspace from actors who are operating with evermore sophistication, speed, and precision. Those are the words of Admiral Rogers.

As with every cyber hearing this committee has held in recent years, we heard how the lack of a strategy and policy continues to undermine the development of a meaningful deterrence in cyberspace. The threat is growing. Yet, we remain stuck in a defensive crouch, forced to handle every event on a case-by-case basis and woefully unprepared to address these threats.

Our hearing today brings together some of our Nation's most experienced and thoughtful national security leaders to help us better understand our cyber deficiencies but, even more importantly, to better understand how we can begin addressing these deficiencies.

A long list of fundamental policy questions remains unanswered.

What is our theory of cyber deterrence, and what is our strategy to implement it?

What is an act of war in cyberspace?

What are the rules of engagement for responding when attacked?

Who is accountable for this problem, and do they have sufficient authorities to deliver results?

Does over-classification undermine our ability to talk openly and honestly about cyber deterrence?

How should we address issues of sovereignty that may or may not apply to data as it moves from country to country?

What about cyber collateral damage?

Organizational questions are equally unresolved.

Should we have a cyber service?

What is the long-term relationship between Cyber Command and NSA [National Security Agency]?

How should we organize our efforts in the interagency?

Who are our cyber first responders?

No matter how well organized and prepared the Department of Defense may be, glaring gaps in our national cyber policy, strategy, and organization undermine our ability to defend the homeland and deter those seeking to undermine our national security in cyberspace.

While we remain stuck, others have made considerable progress in policy formulation and organizational alignment. For example, the United Kingdom recently established its National Cyber Security Centre, a centralized organization that brings the disparate organizations across the British Government under one roof sitting side by side with industry. I look to the views of our witnesses as to whether we should consider a similar organization in the United States.

Another model worth consideration is an organization akin to the U.S. Coast Guard with its flexible mix of law enforcement and military authorities.

Today we lack true cyber first responders. Neither the Department of Homeland Security nor the Department of Defense know who should arrive first on the scene to stabilize and assess a major cyber attack. We should consider developing a Coast Guard-like hybrid organization that can defend our territorial cyber boundaries, be our first responders, and if necessary, gracefully transition and support DOD [Department of Defense], DHS [Department of Homeland Security], or FBI [Federal Bureau of Investigation], depending on the situation.

Each of our witnesses have written or spoken extensively on how cyber has and will continue to shape our national security. We look forward to hearing more from each of you about the actions we can and should take to defend our Nation in cyberspace.

Senator Reed?

STATEMENT OF SENATOR JACK REED

Senator REED. Thank you very much, Mr. Chairman. I want to join you in welcoming our distinguished witnesses and in holding this important hearing.

General Clapper, General Hayden, Admiral Stavridis all have significant experience and expertise in cyber from their service in the military, the intelligence community, the private sector, and academia. We thank you all, gentlemen, for your service to the Nation.

Russia's campaign last year to influence our election undermined faith in our democracy, and the objective truth of the news has been matched or surpassed by its years' long efforts to undermine democracy and the free press in Europe, the NATO [North Atlantic Treaty Organization] alliance, and European unity in general. Russia's ambitious and aggressive use of information as a weapon adds a whole new dimension and urgency to the task of confronting and deterring hostile actions through cyberspace.

We heard testimony 2 days ago from Admiral Rogers that the Russians are still actively trying to influence our domestic politics and are very likely to attack our midterm congressional elections next year. There is not a moment to lose in addressing this challenge to our national security.

However, as Admiral Rogers also acknowledged earlier this week, Cyber Command's Cyber Mission Forces are neither trained nor tasked to operate in this cognitive dimension of information warfare.

By the same token, the elements within the Defense Department that are responsible for information operations have no cyberspace responsibilities or expertise.

This disconnect is replicated across the other disciplines that make up the totality of information warfare and across multiple organizations in the Defense Department and the interagency process.

Additionally, I would like our witnesses to consider the advice of the Defense Science Board task force on cyber deterrence. Prominent former officials such as former Under Secretary of Defense for Policy Dr. James Miller served on this task force and have testified to this committee twice this year. They advocate rapidly developing the ability to conduct operations through cyberspace to threaten, quote, what key leaders on the other side value the most, close quote, which in the case of Russia could include their own financial wellbeing and status in order to deter influence operations and cyber attacks against us.

The threats that we face call for leadership and action. To date, however, despite the many large-scale and impactful cyber events of recent years, the executive branch has not acted to create an effective, whole-of-government capability to defend against and ultimately deter damaging cyber attacks. Congress, challenged by the overlap of committee jurisdictions and concerns of numerous outside stakeholders, has also been unable to design and impose the comprehensive solutions that this problem requires.

However, it is imperative that there be a renewed effort. We must fashion an effective, integrated, and coordinated capability to detect and counter the kind of influence operations that Russia

now routinely and continuously conducts. Likewise, we must act to ensure that our military and the government as a whole has a strategy and capability to deter such actions through the demonstrated ability conduct our own operations of this type. We must also act to bolster the resilience of our society in the face of attempts to manipulate our perceptions and our decision-making.

I know that each of you think deeply about and have recommendations to address these critical issues. I look forward to your testimony and discussion of these urgent matters.

Thank you very much.

Chairman MCCAIN. General Clapper?

STATEMENT OF HONORABLE JAMES R. CLAPPER, JR., SENIOR FELLOW AT THE BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS AND FORMER DIRECTOR OF NATIONAL INTELLIGENCE

Mr. CLAPPER. Chairman McCain and Ranking Member Reed and members of the committee, first I think I want to commend you for your sustained interest in this subject of cyber and cybersecurity and what we as a Nation should be doing about it.

It is certainly an honor to be on the same panel with the likes of Jim Stavridis and Mike Hayden, both old colleagues and friends.

I had some introductory comments about the threat, but I do not think I will dwell on that in the interest of time.

Chairman MCCAIN. Before you leave the threat, though, General, would you say the threat is worsening, the same——

Mr. CLAPPER. I do. Since you have asked me, one of the themes that I have talked about in my former capacity at worldwide threat hearings, to include the last one we had here, was the fact that we in the past have taken some comfort in the fact that the entities which can do us the most harm, meaning Russia and China, probably have perhaps lesser intent, and then the entities which have more nefarious intent, meaning terrorists, criminals, et cetera, have lesser capability. The problem is that gap between the two is closing. The terrorists, criminals, et cetera, hacktivists are going to exploit the technology. That comfort that we may have taken in the past I do not think is something we should count on. So that is an overall comment about the threat. So the short answer to your question is yes.

The other comment I would make is I think what to do about all this transcends the Department of Defense and the intelligence community. We have a huge education challenge getting both institutions and individuals to practice common sense cybersecurity, sort of like the same way that we habitually lock our doors and windows, brush our teeth, or hopefully wear seat belts. There is not that mindset certainly at the individual level or the institutional level.

In response to your request for thoughts on policy, strategy, and organization, I want to offer one overarching thought. To me, the first order of business is defense and resilience. We got to focus on this because without it, we will never be in a position to launch a counter-attack even if we can quickly and accurately attribute who attacked us which, by the way, is not in itself a trivial task. We are always going to doubt our ability to withstand a counter-retal-

iation. I saw examples of this during my time as DNI [Director of National Intelligence].

One case in point. When the Iranians launched a series of denial of service attacks against our financial sector—I think it was in 2013 or so—the initial interagency impulse was to counter-attack but in a measured, precise way. What restrained us was lack of confidence in our ability to absorb a counter-retaliation. We could not be sure it would be similarly measured and proportional and legalistic, which is the way we do it, or what the second order or third order or unintended effects might be.

So we have to recognize and accept that it is inevitable that we are going to be attacked, and the real issue is how resilient can we be to recover. In the absence of that resilience and the confidence it gives us, it will continue to inhibit our responses.

This imperative on defense and resilience applies not just to the Federal Government at large and to DOD and the intelligence community but applies equally to people sitting in the White House situation room or board rooms. So defense and resilience must, in my view, be the pillars of whatever policies and strategy that we adapt. That to me is the very foundation for deterrence.

A related point—and I have said this before—is I think accordingly we should use all the tools potentially available to us, diplomacy, economic sanctions, and other forms of military power, when we consider responses to cyber threats. Just because someone attacks us using cyber should not automatically mean that we should respond the same way. In fact, if the adversary chose cyber because it asymmetrically favored them, responding in kind means we are sort of letting them define the terms of the engagement and fighting on their terms. Of course, intelligence, by the way—I would mention this—has a crucial role to play in identifying ways to leverage a cyber adversary.

With respect to the current posture of the U.S. Government, I would say—my mild understatement—it is not very good. Still, many organizations across the government have old, hard to defend IT [Information Technology] architectures, and certainly the OPM [Office of Personnel Management] breach got everybody's attention but it is probably the tip of the iceberg.

One trade publication recently reported that 34 percent of U.S. Government agencies surveyed experienced data breaches in the past year, and 65 percent reported experiencing a data breach at some time in their history. These agencies cited old systems, lack of funding, and staffing shortages as the cause.

The Trump administration, I understand, is preparing a new executive order on strengthening the cybersecurity of federal networks and critical infrastructure. It emphasizes accountability, managing the government IT architecture as a federated enterprise, and all that. What I expect is, though, that the accompanying authorities and resources will not match these bold goals.

This leads me to another crucial point. Even if the agencies in the government complied with this forthcoming executive order, both the spirit and substantively, we will still have no recognized standardized way to measure whether we are more secure or not. To me, this is a major deficiency that must be addressed. The term "cyber metrics" applies to at least six different dimensions of cyber.

Do we measure compliance with standards or how much we are spending or what functions we are performing or how we gauge the threat or calculate risk or measure return on investment? There is no consensus on any of these six ways or some combination thereof to measure whether we are actually improving cybersecurity.

On organizational things, you asked about the suitability of the Federal Government's organizational structure. Here I will probably, I am sure, present a contrarian view to my colleagues.

As a general comment, the older I have gotten, the less appealing reorganizations are to me. I say this both as a victim and an instigator of reorganizations. Big ones are hugely disruptive and distracting and take years to gel. The way the government is organized now can work provided that each component has the authorities clearly defined and the resources to perform its mission. So I do not have any big, lofty ideas on reorganizing the government's approach to cyber.

I do, however, have two related organizational comments that are maybe less lofty but to me important.

First, I feel compelled to repeat something I said last January when I appeared here on the 5th of January, and that is my strong conviction about separating Cyber Command and NSA. If you invite me here to speak about cyber, I am always going to bring that up. NSA is a crucial component of the intelligence community, and I do not believe it is healthy for it to be essentially subordinated to a sub-unified command of DOD.

I was the Under Secretary of Defense for Intelligence when we came up with this arrangement and had a lot to do with it. I believed in it at the time. But it was never intended to be permanent. This was 7 or 8 years ago.

So I would urge the establishment of a date certain to separate and then work to make it happen. NSA will always have to provide support to the Command, but I believe an intelligence agency director should be focused full-time on the mission of their agencies. Again, I repeat NSA is a crucial part of the intelligence community.

The Commander of CYBERCOM [Cyber Command] and Director of NSA are each a full-time job. If CYBERCOM is elevated to unified command status, which I believe it should be, then separation is even more urgent. As the late Johnnie Cochran might say, if you elevate, you must separate.

Second, I do not support establishing a separate cyber service in the military, just as I am not a fan of having a separate space service. I think such proposals, if implemented, would create even more stovepipes, complicate personnel management, and I think make career progression for the people in it harder.

Finally, I have three brief comments on cyber issues in the intelligence community which maybe are a self-criticism.

First, the intelligence community needs to strengthen how it reports cyber intelligence to users with differing perspectives and needs. This means providing reporting to policymakers that is timely and relevant but not head-hurting technical and importantly identifies the so-what implications for action. Intelligence needs to move from reporting cyber anecdotes to a systematic framework that focuses on trends and the big picture.

Secondly, the IC needs to improve its support to state, local, tribal and private sector entities. This requires a better understanding of them and what their needs are. There are probably three kinds of customers for cyber intelligence, policymakers, line or core business people, and IT staffs, which are kind of like the military categories of strategic, operational, and tactical. I think it would be useful if the IC kind of thought about how they relate to the various customer sets using that analogy.

Third, an always hardy perennial recommendation for the intelligence community is to enhance information sharing. This gets to your point about classification. Yes, we over-classify. No question about it. All I ask, though, is that when we look into this, we do consider the equities from the standpoint of the intelligence community. If we are going to declassify, transparency is always a double-edged sword. It is good but adversaries go to school on that transparency.

The other point I would make here is that information sharing has got to be a two-way street. The private sector is often the first to know of a cyber attack, and so rapid sharing must work both ways. Companies cannot depend on the government to provide just-in-time warning that its intellectual property clock is about to be cleaned. There are some understandable inhibitions on both sides that prevent this, but we must do better.

So with that, I will turn to, I guess, Admiral Stavridis. Thank you.

STATEMENT OF ADMIRAL JAMES G. STAVRIDIS, USN, RETIRED, DEAN OF THE FLETCHER SCHOOL OF LAW AND DIPLOMACY AT TUFTS UNIVERSITY AND FORMER COMMANDER, UNITED STATES EUROPEAN COMMAND

Mr. STAVRIDIS. Good morning. Chairman McCain, Ranking Member Reed, members of the committee, again thank you for asking me to come down and speak.

I think we are facing potentially the most disruptive force in this cyber world, and we have a gaping vulnerability in my view.

I do want to mention that in the course of the panel, I think we are probably not going to agree on everything, but you will be pleased to know we coordinated our hairlines for disagreeing.

[Laughter.]

Chairman MCCAIN. I know how you feel.

[Laughter.]

Mr. STAVRIDIS. You look like a potential donor to me, Senator.

[Laughter.]

Mr. CLAPPER. Grass does not grow on a busy street. Or as my wife is quick to remind, nor out of a concrete block either.

[Laughter.]

Mr. STAVRIDIS. So I will talk very briefly about kind of three threat vectors. One is pretty obvious. It is national security. This is what General Clapper has outlined for us. I think the commercial sector is second, and then thirdly we should recall there is a very personal vector to cybersecurity that potentially influences each of us as you think about what that super computer you are carrying around in your pocketbook or purse say about you. So those three vectors I think are merging in a dangerous way today.

There are 7 billion people on the planet, probably 20 billion devices connected to the Internet of Things. Fairly recently we just saw an attack that turned the Internet of Things into an Internet of Botnets, creating real havoc in a variety of crucial commercial sites. We have seen hundreds of millions of accounts hacked, most recently Yahoo. We have seen multiple actual thefts occur, $87 million from the Federal Reserve Bank trying to get money from Bangladesh to the Philippine Islands.

On the national security perspective, we see attacks, I would argue, from North Korea, Russia, certainly brushing up against attacks from China. Iran I would categorize an attack. These vulnerabilities come together in two fundamental points. We are deeply challenged. As both the chairman and the ranking member have said, and as General Clapper has said, we are not particularly well organized. Yet, we as the United States have the largest threat surface of any nation in the world.

So what do we do about it? I will launch a few ideas. All of these ought to be considered as modest proposals at this time. These are things we should think about doing and have more conversation about.

One I would say I am firmly in favor of—and I am going to agree with General Clapper on this one—I do believe that the NSA and Cyber Command should be separated. I have been speaking and writing about this for several years. To me, the jobs are too big. The missions are different. The span of control is a deep concern and rising. I think Cyber Command should be elevated to being a full combatant command and, as the General says, separated, and I think probably two fundamentally different leaders are needed at those two commands.

Secondly, the idea of a cyber force. Here I am going to disagree with General Clapper. I think we should take a serious look at it. What I try and do at times is reach back into history, and I am mindful that I am flanked by two Air Force generals. If we were having this hearing about 100 years ago, the Army and the Navy would be adamantly saying, hey, we do not need an Air Force. Why do we want that? We can handle that. Yet, today I do not think we could imagine our military functioning without all that the Air Force brings to the table. I think cyber is kind of like that, and I think in 100 years we will look back and say, boy, were we really having a debate about whether or not to have some kind of cyber force?

So I would say let us take a serious look at this, whether it is a separate force in the same model as the Army, the Navy, the Air Force, the Marine Corps, perhaps not. A Coast Guard model I think is a very intriguing way to think about this. But I think at a minimum this would be something the Congress would be interested in hearing more views about and recognize, again, looking to the history of the creation of the U.S. Air Force, you are going to get enormous pushback from the Department, from the individual services. I know Admiral Mike Rogers was just up testifying, disagreeing with the idea as well. Fair enough. Let us bring that debate on.

A second idea I think that is worth thinking about at least is being more demonstrative of our offensive cyber capabilities. I think that would help create more deterrence if we did so.

I agree with General Clapper. We do not need to reach into the cyber toolkit every time we are cyber attacked. But I think in our zeal, appropriate enough, to try and protect the nature of our cyber tools and our sources and our capability, we can lead some to underestimate our ability to retaliate. Eventually we are going to have to build a deterrent regime of some kind. We ought to be having a coherent conversation about levels of classification and how we would want to do demonstrations.

Fourth I would say doctrine. This is always kind of the military bugbear in me. But what is the definition of a cyber attack? I think it is time we really grappled with that, and on a spectrum that runs from nuisance defacing of websites to kinetic demonstrations that actually kill people and destroy massive amounts of material and equipment, somewhere on that spectrum lies what we ought to think about as a cyber attack. I would argue what North Korea did to Sony Pictures, an American corporation, which included kinetic damage and a high degree of business and economic damage does, in fact, verge into an attack, not as was categorized at the time as cyber vandalism.

Sixth—and then I will kind of stop there because you asked specifically about this—organizing the government. Taking Director Clapper's views about skepticism of both reorganizations and creation of new bureaucracies, I will put it this way. I think there needs to be a voice in the cabinet that focuses on cyber. Now, you could take the Director of National Intelligence and make that the Director of National Intelligence and Cybersecurity, for example. You could have a new department. We have a Department of Agriculture, a Department of the Interior. These are important organizations, but they reflect where we were as a Nation 150 years ago. The idea of having a dedicated voice in the cabinet talking about cyber has appeal to me.

I will conclude by saying I had a wonderful career in the military. Now I am an educator. I am the Dean of the Fletcher School of Law and Diplomacy at Tufts University. I have come to value education even more.

I will close with something the Director said at the beginning. 65–70 percent of the cyber intrusions and attacks occur because of bad cyber hygiene, which is bad cyber education. The more we emphasize science, technology, engineering, math, computer science, coding, the more we have an informed population, the better protected we will be. That may be the most important thing we can do of all.

Thank you for listening to a few ideas. I will close by saying, because I have two Air Force generals with me, in the world of cyber, we are kind of on the beach at Kitty Hawk. We have got some work to do ahead of us. Thank you very much.

[The prepared statement of Mr. Stavridis follows:]

PREPARED STATEMENT BY ADMIRAL JAMES STAVRIDIS

Thank you for the invitation to appear before you today to discuss the most disruptive force facing America's military and society today: the rapid emergence of

cyberspace as an operational domain for armed conflict, as well as a gaping vulnerability in our commercial, financial, and infrastructure systems. I commend the members of this Committee for their continued commitment to advancing America's defense interests in cyberspace, and I ask that my remarks, which were provided to the committee previously, be entered into the record.

I am honored to appear with two Air Force Generals whom I have known and deeply admired for decades. You may also note this is a panel that may not always agree on our views and but we have managed to coordinate our hairlines.

Cyberspace is indeed a new domain of warfare but it is one unlike sea, air, and land in that it is not physically traversable by our sailors, airmen, and soldiers. The digital battle space of the twenty-first century is not marked by geographic landmarks or public infrastructure, but rather operating systems, routers, switches, and servers—most of which are designed, manufactured, owned and operated by both American and international companies and citizens, i.e. the private sector. As a nation we are under-educated in these systems, and few could actually explain how an email gets from their iPhone 7 to their grandmother's iPad. Yet these systems are highly at risk at every level, from our national security—proven by well-documented attacks from Iran, North Korea, China, and Russia; in our commercial sector, with cyber crime rising rapidly and approaching perhaps hundreds of billions of dollars globally on an annual basis; and indeed in the most intimate details of our personal lives, which are far-too-often carried unprotected in the super computers we casually carry in our pockets and purses. Of all the threats our nation faces, only cyber cuts across so many dimensions.

There are 7 billion people on the planet, but perhaps 20 billion (or more) devices connected to the Internet. As we saw during the recent attack on Dyn, the internet of things became a "botnet of things" creating significant commercial havoc and threatening consumer confidence in the security and reliability of commoditized online services. There are 23 victims of malicious cyber activity per second according to a 2016 report from Norton, and many studies suggest that damage to our national economy approaches $200 billion per year. We have seen North Korea, China, Iran, and Russia—among other nations—attempt to penetrate of cyber defenses and conduct a wide variety of espionage, commercial damage, data manipulation, and kinetic destruction to infrastructure. The Department of Justice has brought indictments against agents from all of those nations

Because we are under-educated and lightly protected, offensive cyber actors, comparatively large in numbers and concealed by the identity-obfuscating properties of cyberspace, enjoy a significant advantage over the defense, which, in the United States, is necessarily constrained in its maneuverability to protect our citizens' privacy and civil liberties.

Today, therefore, I would like to preface my opening comments by declaring two seemingly obvious but fundamental truisms that I would suggest inform the Department of Defense's and the Nation's cyber policies and strategies in this decade and beyond.

First, the United States military is today deeply challenged in preventing destructive cyber attacks against the nation from capable adversaries, to include state and non-state actors. While we have made progress, we have not trained, equipped, and organized ourselves to be safe in cyber space.

Second, and closely related, the United States is undoubtedly most visible, exposed and lucrative target Nation in this new military domain and therefore subject to disruptive and destructive attacks from not just well resourced nation-states and sophisticated criminals, but also jihadist and other terrorist organizations.

Given these basic facts, the Department's cyber posture must shift from one that is primarily focused on mitigating and defending from malicious cyber activity to one that also aims to deter state and non-state adversaries and belligerents in cyberspace while reducing the threat from lower level actors. Raising the barriers to entry for bad actors will require a stronger and more robust military capability; better organization within the US government at the cabinet and agency level; higher levels of societal education about the risks and concerns we face; better technology and equipment; and a vastly improved level of private-pubic cooperation. Overall, we must make it harder, costlier, and more time intensive for our adversaries to effectively operate in cyberspace.

Creating real deterrence in cyberspace against opposing national actors will be challenging. If we can agree that deterrence is the combination of both capability and credibility, it is clear that we have work to do on both fronts.

In terms of capability, we have extraordinary offensive and defensive cyber tools, but we must continue to improve as our opponents are doing so rapidly. I would argue that it is also time to strongly consider whether or not we want to create a dedicated cyber force.

While the individual services today—Army, Navy, Marine Corps, Air Force and Coast Guard—are working hard, they are like five horses who can often pull in slightly different directions. Unfortunately the current distributed force structure across each of the services not only breeds redundancies, threatens unity of command, and fosters unproductive competition within the Department, but it also dilutes the increasingly rare and therefore precious core competencies of our cyber planners, operators, trainers, and commanders.

United States Cyber Command declared Full Operational Capability (FOC) in 2010 and seven years later, despite the valiant and well-intentioned efforts of Admiral Mike Rogers and his predecessor, General Keith Alexander, the Cyber Mission Force has demonstrated to be a less than formidable and sustainable model. Most recently, of the 126 airmen who completed their first tour with the Cyber Mission Force, zero were retained for a second tour. In other words, all 126 airmen were assigned to other Air Force missions with no cyber nexus whatsoever. In this regard, establishing an independent cyber force would constitute a show of force—sending a message to our allies and adversaries alike that the United States is committed to recruiting, retaining, and training cyber warriors not just for a single tour but for a career—one that is in some ways traditional to military life and in other ways wildly different and perhaps more representative of life at a Silicon Valley start-up.

From an historical perspective, we have stood at this moment before, roughly a hundred years ago, as we contemplated another new medium in which combat would occur: the air. The Navy and Army fought the idea of an Air Force for decades until forced to concede after Congressional action. Today, and I think my esteemed panelists would agree, we cannot imagine our joint warfighting capability without a US Air Force. It is time we at least began a conversation about a US Cyber Force. The idea will be vehemently opposed by the services, just as the Army and Navy fought the idea of an Air Force. But sooner or later, common sense tells us we will end up with a specialized force in this zone of combat.

I will also observe that many of these same arguments would apply to both Space warfare specifically and Information Dominance broadly. It is certainly worth exploring whether a Cyber force, a Space force, or a broad Information Dominance force makes the most sense. Chairman Rogers in the House gave a powerful and sensible speech on the space aspects of this. Since we are looking today at Cyber, I will keep my arguments focused on a cyber force; but I freely admit this is a broader question that encompasses space and information dominance together.

A good model to consider as a "starter step" for a cyber force would be to fully make Cyber Command independent and then use the Special Forces model—a defined budget, specialized operators form the services (think SEALS, Rangers, Green Berets, PJs, and Recon Marines), but a defined career path in Cyber much as a Navy SEAL largely has a defined operational career path in the Special Forces. Over time, we may want to shift beyond this to a full blown individual service.

This could start relatively small, with numbers in the 5–10,000 range, a lean administrative structure, and connectivity to the larger services.

The Congress may want to task the Department of Defense with studying the idea and reporting on the options worth considering. The administrative path of Goldwater-Nichols may be instructive.

While standing-up a U.S. Cyber Force would constitute a major step towards establishing a credible deterrent, it is not sufficient by itself. In addition to signaling our long-term commitment to defending our interests in cyberspace, we must also signal both the capability *and* the will to project cyber force across the globe. For this to happen, we must satisfy two conditions.

First, we must somewhat lift the veil off of military cyber operations. I have no doubt that the United States' Armed Forces boasts some of the most advanced, if not *the* most advanced, cyber capabilities in the world. But if we refuse to demonstrate or even acknowledge this capability we are only encouraging aggression from other, less capable actors against our highly vulnerable infrastructure. In a world in which the number of networked devices exceeds the world's population by more than three fold, we simply cannot afford to confine cyber operations to the covert toolkit. To the contrary, cyber operations are a legitimate means of projecting national power, especially when proportionately supplemented by kinetic force, and we should advertise them accordingly.

In addition to shedding light on our non-kinetic military capabilities, we must convince the world that we, despite living in a glass house, are not afraid to throw stones. Interestingly, the United States' unwillingness to operate offensively in cyberspace is driven less by a fear of retaliation and more by a fear of compromising our Intelligence Community's sensitive tradecraft. The diminished stature of United States Cyber Command as a Sub-Unified Combatant Command (COCOM) under

United States Strategic Command, combined with its institutional, leadership, and technical ties to the National Security Agency (NSA), has limited our Armed Forces' cyber freedom of maneuver in support of military objectives.

We should also increase our work with allies, many of whom are quite adept in this sphere. In addition to NATO partners like the UK, France, Germany, and Estonia, other nations with significant ability include Israel, Japan, South Korea, Singapore, Sweden, Australia, and others. Cyber security is a team sport not only in the interagency, but within our international alliances and coalitions.

Related to this, the Department must embrace and employ an agile software development lifecycle and mindset that accommodates development sprints and high rates of failure. These methodologies, tested and proven in the private sector, will enable our cyber warriors to keep pace with what is certain to be a more fluid and dynamic operational tempo than ever before.

It is also imperative that the Department establish a solid doctrinal foundation. The policies governing how our military operates in cyberspace will likely change many times over in the next decade, but we must quickly establish a common vernacular—not just within the Pentagon but across the national security apparatus and the government as a whole. For starters, we must not diminish the many forms of cyber aggression our governments, companies, and citizens are experiencing. Consider, for example, the Sony hack in 2014 reportedly attributed to North Korean and dubbed an act of "cyber vandalism" by former President Obama. "Cyber vandalism" is defacing a webpage over an ideological difference; the Sony hack could certainly be considered as an act of war—in addition to millions of dollars of kinetic damage to Sony's hardware, a high level of business value was destroyed. While no one died, the damage was significant. We, of all Nations, cannot afford to understate or diminish the significance of force projection in cyberspace. We need to create a "definition of a cyber attack," which differentiates among surveillance, espionage, commercial interference, data modification and manipulation, data destruction, infrastructure attack on critical infrastructure, kinetic damage, and loss of human life.

We should be thinking more holistically about how the US government conducts cyber security and the role of the Department of Defense in that mission. Today, cyber security falls under a plethora of different cabinet departments—DHS, DOJ (FBI), DOD (NSA), and DNI. There are six different cyber security centers run by the US Government. We have a Secretary of Agriculture and a Secretary of the Interior in the Cabinet, but not a single voice for Cyber. There are a number of ways to address this, from a Department of Cyber that fuses all of those functions and centers (much like the British have done with the creation of their National Cybersecurity Centre NCSC, embedded in GCHQ) to giving a unifying voice to one Cabinet Secretary (perhaps the DNI becomes the DNIC, Director of National Intelligence and Cyber Security). Many of these ideas were explored by the Commission on Enhancing National Cybersecurity, led by fomer National Security Adviser Tom Donilon—I endorse many of its findings. As a side note, I think it is also time to strongly consider splitting the positions of US Cyber Command (a military warfighting Combatant Command) and the Director of the National Security Agency (fundamentally an intelligence gathering operation, although also invested with cyber activities both offensive and defensive). The span of control and differing missions makes continuing to merge those in one person—even one as good as the two officers with me today or Admiral Mike Rogers—less than optimal. Bottom line—we are not organized to seamlessly defend or fight in cyberspace as a nation and have a great deal of work to do, both as a nation and within the Department of Defense.

Finally, as an educator myself these days, I cannot resist making a comment about the role of education in increasing our national security and indeed our own efficiency within the Department of Defense. We have to improve all level of Science, Technology, Engineering, and Math in our educational system, of course; but there needs to be particular emphasis on the practical skills of cyber as well as understanding how to defend ourselves individual. Over 70% of all hacks, intrusions, cyber crimes, and so forth result from simple failures in cyber hygiene. This is true for society at large and the Department of Defense. More emphasis on this aspect is like "soft power" in the context of national strategy—it is preventative, cheap, and has enormous ancillary benefits. While not specifically under the purview of this Committee, it is something the Congress can be influential in pushing and would go far toward helping with the overall mission of cyber security.

In so many ways, in the world of cyber security we are still "on the beach" at Kitty Hawk to use an aviation analogy. Or to shift to a maritime one, we are sailing in very choppy seas. The Congress can play an important role, as it has historically, in helping the Department of Defense and the rest of the Federal Government to improve all elements of our security.

Again, thank you for asking me to come and testify. I am happy to answer any questions the Committee may have.

Chairman MCCAIN. General Hayden?

STATEMENT OF GENERAL MICHAEL V. HAYDEN, USAF, RETIRED, PRINCIPAL, THE CHERTOFF GROUP AND FORMER DIRECTOR, CENTRAL INTELLIGENCE AGENCY

Mr. HAYDEN. Thank you, Mr. Chairman, Senator Reed. Let me, first of all, violently agree with the diagnosis that both of you laid out in your opening comments. I think you have got the symptoms we are trying to treat here exactly right.

I first encountered this cyber thing more than 20 years ago. I was pulled out of Bosnia, a war that was essentially medieval in its conduct and in its causes, and parachuted into San Antonio, Texas at the Air Intelligence Agency, which was actually on the cutting edge of thinking about cyber then. I still remember the introduction I got from my staff. They never quite said what I am going to tell you now, but if I boiled it down, it was, General, we are glad you are here. Take out a clean sheet of paper and a number 2 pencil and write this down. Land, sea, air, space, cyber. It is a domain. It is a theater. It is a location. It is not bandwidth. It is not a budget line item. It is a place where we are going to go and operate. By the way, I think that is exactly right and it is now American military doctrine.

I think what we are debating for the next 20 years is what of our life experience and lessons in these domains transfer or do not transfer into this new cyber domain. So, Senator, you mentioned questions of sovereignty or what is an act of war, what is legitimate state espionage, what are the principles of deterrence. I could go on. But there is really no consensus yet even within the armed forces as to what experience here still applies up here.

I think one of the reasons we lack consensus is as a Nation, not just as a military, we lack policy because we lack consensus. We lack consensus because we have not had that adult discussion that we need to have, and we have not had the adult discussion because frankly I do not think we have a common view of the reality, a common view of the battlespace. That is inhibited, as has already been mentioned by both of you and by General Clapper, by the lack of knowledge, information in this space, over-classification. Before I focus exclusively on the government, let me include industry in that as well because they keep the ball on their hip a lot of times too for their own purposes. I do think we need to have far more openness as to what goes on, what our capabilities are, what the threats are, and frankly, exactly what happened.

General Clapper just mentioned the Iranian attacks against the banking system in New York, massive denial of service attacks, but something our government will not go out of its way to actually say has happened with the clarity that Jim had just used.

Part of the over-classification problem—and General Clapper and I probably share guilt here—is that our cyber thinking in the armed forces and in the government is rooted in the American intelligence community. If this had been developed at another part of our structures, I think a lot less of this would be on the other side of the door and a lot more would be open. Of course, without

consensus on policy and these basic foundational definitions, the organizational structures that should follow that is always in flux, always subject to debate.

I was, to be fair, present at the creation when we decided to put a Title 10 warfighting function at Fort Meade. It was not quite Cyber Command then. It was Joint Functional Component Command Net Warfare, but I am the first Director of NSA who actually had Title 10 warfighting abilities and authorities under Strategic Command.

Even when we did that—and I still recall briefing the Chairman of the Joint Chiefs of Staff and he turned to me—it was General Dick Myers, whom I had known for a long time—and said, Mike, is this going to solve this. My response was, oh, no, sir, not at all, but we will be back to you in a couple years messing this up at a much higher level than we are currently. That has been the evolution. As we develop technology, a trained workforce, a deeper understanding, the structures will change as our understanding changes.

Let me join consensus here. I think there is a point in time—and I do not think it is very far away—where the structures have to adjust to changing capacities and Cyber Command and NSA have to be separated. That is not a panacea. It is not the philosopher's stone. It is not going to turn digital lead into digital gold for us, but I think it is a powerful step forward.

Senator McCain, I was really intrigued by your comment about perhaps the U.S. Coast Guard is a workable model. I actually joined an effort by the American Enterprise Institute about a year and a half ago that actually tried to seek how should we organize as a government not just as the armed forces to deal with the cyber domain. The Coast Guard model really does offer some interesting examples. It is an educational organization. It is dedicated to public safety. It is a first responder. It conducts search and rescue. It is a law enforcement element of our government and in extremis, we can use it as a combat arm of the American Government. Obviously, it does not transfer perfectly, but I do think there is some really interesting parallels here that we could profit from as we try to move forward and create a whole-of-government response.

Again, one more time, let me join consensus. The Coast Guard is an intriguing model because it straddles government and private sector. We really do have to do that in terms of cybersecurity. So any model that allows us to put our arms around the private sector where, frankly, I think most of these battles will be won or lost, is one that we should pursue.

I look forward to your questions and learning a great deal from my colleagues here.

Chairman MCCAIN. Do you think the private sector is eager to cooperate?

Mr. HAYDEN. The private sector gets it as victim. This is life experience. I am out of government 8 years now. When I first started talking with them, we were a nuisance talking about cybersecurity. They now know that cybersecurity is not a subtraction from the bottom line, but it is integral to the top line. That part they get.

What they have not yet embraced is that they could enter into a deeper relationship with the government that would not inhibit

either their financial or their cybersecurity success. The burden of proof might be a bit more on us than on them.

Chairman MCCAIN. I get the impression that a lot of these particularly major Silicon Valley corporations would like to stay as far away as possible from the Federal Government.

Mr. HAYDEN. Senator, we are probably still feeling the after-effects, the second and third order effects, of the Snowden revelations and so on. I would have agreed with you more strongly 2 or 2 and a half years ago, but in my recent dialogue with them, I do see a shift. Let me give you an example.

I will be a little oblique here. Vault 7, which was allegedly an awful lot of CIA [Central Intelligence Agency] cyber tools going public. We have not seen Silicon Valley rending their garments in outrage about this. I think their response to this has been far more mature, far more understanding of the appropriate role of government than we saw 2 or 3 years ago.

Chairman MCCAIN. Thank you.

I take it our witnesses agree that until our adversaries believe the consequences of an attack in cyberspace will outweigh the benefits, behaviors will not change.

Mr. STAVRIDIS. Yes, sir.

Mr. CLAPPER. Yes, sir.

Mr. HAYDEN. Yes, sir.

Chairman MCCAIN. Every event is being handled on a case-by-case basis. Is that appropriate or sustainable?

Mr. CLAPPER. That is true, but I think that is a swing at me from the prior administration. Every case is a little different, at least for the cases we encounter. It would be nice to have a broad policy, though, that you could start with, which we really do not have.

Mr. HAYDEN. Let me go deeper than Jim. In the Bush administration, we could not do a cyber thing without having a meeting in the situation room.

Chairman MCCAIN. What are the impediments? There is a common refrain here, constant refrain, we do not have a strategy, we do not have a policy, therefore, we have huge problems. What is the impediments here? What is keeping us from—the last administration and then the administration before that were all good people. They all understood the threat, but yet, we have not developed a policy or a coherent strategy. Is it a lack of leadership? Is it a lack of focus? Is it a lack of evolving technologies? What is the problem here? I am not sure we can solve it without defining the problem.

Mr. CLAPPER. I will take a try at that, although I do not think it will be satisfactory to you, Senator McCain, is what I tried to get at in my statement about lack of confidence in our ability to absorb a counter-retaliation. That is why to me, if you are going have a serious discussion about deterrence, the fundamental underpinning of deterrence has got to be defense and resilience. Unless we are confident that we can withstand a counter-retaliatory action, which may not be as measured and precise as we might employ, having a serious discussion and writing things down in the absence of that is pretty hard.

The other thing I ran into, not to sound like an excuse here, but are legalities. I think Jim mentioned the Sony attack. Of course, putting aside the issue of whether that impacted the national security of not, the First Amendment I guess, so if we consider only using the single domain of cyber to retaliate, then the issue comes up, well, we have to execute and attack through someone else's infrastructure in order to get ultimately at the target. Is that an act of war against that intermediary or not? Lawyers have a field day with that kind of an issue.

So in the end, in the case of Sony, we ended up not doing anything in the cyber domain but using other tools, sanctions against North Koreans, which for me were ceremonially satisfying but really did not have a lot of impact.

So those are the complexities. It sounds legalistic and bureaucratic, but to me, those are the kinds of things that have inhibited us.

But the main point I would make is that unless we have confidence in our ability to absorb an attack and be resilient, it is always going to inhibit a single domain response, that is in cyber. That is why I mentioned using all the other tools.

Mr. STAVRIDIS. Senator, if I could, Chairman McCain. I think those are salient points.

I would add back to this theme of education. For the Senate Armed Services Committee, the question becomes are those in the military under the purview of this committee receiving enough computer science. Are each of the academies training to this, the ROTC [Reserve Officers' Training Corps] programs? Over time, I think some of these problems will be solved simply by demographics, as younger people who are digital natives come into positions of authority. But I think that is part of the problem we are trying to solve here.

Mr. HAYDEN. Senator, I would just add one thought. I totally agree with Jim's analysis about our defense. We self-deter because we do not understand how well we could deal with the second and third steps.

But with regard to what is legal, what fits policy, the problem is we do not have any case law. We do not have any generalized recognition of what constitutes accepted international practice.

One way to create accepted international practice is to practice. We actually have the opportunity to establish case law. We have the opportunity to begin to set out what is accepted international practice. I would suggest a country like ours with checks and balances and transparency would be doing the world a service by creating an accepted regime in this domain by prudently using some of the capacities we have.

Chairman MCCAIN. Well, I thank the witnesses.

On the issue of the cyber corps, or whatever you want to call it, I do not know if we ought to establish that. But right now I do not see a clear career pattern and a path to success for these very valuable individuals who have these special talents, maybe not to be a fighter pilot or a tank commander, but to be able to engage in this hand-to-hand combat that we are involved in. Again, I am not sure whether it is a cyber corps, but we better establish a path and in-

centives for people to engage in countering what we all agree is a major threat to American security.

Senator Reed?

Senator REED. Well, thank you very much, Mr. Chairman.

Thank you, gentlemen, for your excellent testimony.

Just a quick follow-up, General Hayden. We can make some law by doing things that are accepted either explicitly or implicitly by the intelligence community. We also can sit down and try to essentially do an agreement. We did it with the financial world after World War II with Bretton Woods. I do not sense any effort anywhere to try to do that. Am I missing something?

Mr. HAYDEN. There has been an effort. Actually Michele Markoff at the State Department, who takes the Acela up to New York routinely and tries to use the U.N. to transfer the accepted laws of armed conflict here and transfer them up here into the cyber domain—and she has been somewhat successful.

Beyond that, though, Senator, I think the real issue we have is there is a big chunk of the world—and some of it comprises our friends—a big chunk of the world who consider cybersecurity preventing that for which we think we have the Internet in the first place, which is the free flow of information. Their definition of cybersecurity is control of data entering into their sovereign space where ours is quite different. We run headlong into this lack of consensus. Hence, my approach to begin to create a normative regime established in essence by practice by a prudent, law-abiding nation.

Senator REED. With respect to a normative regime, as I indicated in my opening statement, the task force on cyber deterrence suggested that we develop the ability to hold at risk key aspects of potential opponents or adversaries, including in some cases the individual wealth or the individual status of potential opponents.

Is that something that is in this concept of trying to establishing the rules of the road, General Clapper?

Mr. CLAPPER. Well, I think what you are getting at—at least it conjures up in my mind, Senator Reed—is the notion of using sanctions, economic sanctions, to leverage identified cyber opponents.

Senator REED. I think you could almost go further than that of using as cyber operations to literally go after the resources and the finances of individuals.

Mr. CLAPPER. Sure, I think that would be useful to have in the toolkit.

Senator REED. Again, going back to the point that General Hayden made, if we have it in the toolkit, we never use it, it is not seen as deterrence. Do we have to use it at some point?

Mr. CLAPPER. Well, yes. Of course, you kind to come to think about why does the nuclear deterrent work. It has so far—knock on wood—for 70 years. But that really is not a very good comparison when you think about it because they are different, and there are only nine countries that have that. The fact that we have not, no one has used nuclear weapons 70 years in itself—and the problem with cyber it is so ubiquitous, it pervades so many aspects, and there are so many things that go into the cyber world that do not merit—you know, they are annoyances, and they do not merit cer-

tainly a nation state response. So those comparisons to me are not very satisfactory.

Senator REED. Admiral Stavridis, your comment.

Mr. STAVRIDIS. Just to pick it up, as I was saying earlier—and I think this is where General Hayden and I are on the same page—using an appropriate, demonstrative, offensive capability can have a wonderfully clarifying effect on the minds of your enemies. I think it is time to lift the veil a little bit. Finances are one thing, I think absolutely. I think another is military forces, not the nuclear forces, though, should be off the table, but showing that we have real capability against nation state actors I think it is time to strongly consider some form of that. Again, as General Hayden says, it builds a regime in international law that I think would be salutary.

Senator REED. Just a final point. I think your comments clearly reveal that we have significant vulnerabilities, particularly on our civilian sector. We have done a lot more for the military, but we could do much more. But when we come to the civilian sector, it is quite vulnerable—our critical infrastructure.

It seems to me there are a couple of paths to pursue. One would be pass laws, regulations, require them to do this or that. Second is to use the insurance market perhaps to get them to include in their operating costs the costs of protection. One element is insurance—we have the terrorism reinsurance initiative, which is essentially designed for structures that might be destroyed. But I think we are getting to a point in the world where the structures are less vulnerable in some respects than the electronic infrastructure. But, again—quickly because my time has expired—are there any thoughts?

Mr. CLAPPER. If I could just foot stomp something that Admiral Stavridis said, which is the huge importance of education. At my headquarters, just ODNI, Office of the Director of National Intelligence—and you know, this is composed of intelligence professionals that understand the threat. Yet, the only way we could improve their sensitivity to spear phishing, you know, a fairly common thing out there, is to test and then throw up the results on the screen once a week at the staff meeting, embarrass the senior leaders about your folks need to be better educated, and we just keep testing and the grade scores would go up. Well, we do not do that. To me, it is just fundamentally important that institutionally and individually, there needs to be better recognition and better education about the threat.

Mr. HAYDEN. Senator Reed, can I just double down on the cyber insurance question?

Senator REED. With the chairman's permission.

Mr. HAYDEN. That unleashes a business case for businesses to actually increase their cybersecurity without the negative effects of a compliance mindset coming out of government regulations. So anything the Congress could do to make that more possible, whether it is second insurer or other aspects of the insurance industry, I think would be a real plus.

Senator REED. Thank you.

Mr. STAVRIDIS. I agree with that, and I want to be on record as such. Thank you.

Senator REED. Thank you.

Chairman MCCAIN. Senator Wicker?

Senator WICKER. Admiral Stavridis, give us an example scenario of how we would demonstrate openly our offensive cyber capability.

Mr. STAVRIDIS. Following an intrusive attack into our electoral process, bank accounts disappear from leading Russian oligarchs who are connected closely to the regime, sort of level C; government officials, many of whom are moving money offshore in Russia, level B; or go after Vladimir Putin, level A. You want to think very carefully as you go up that ladder of escalation, just like you do with traditional——

Senator WICKER. Go after Vladimir Putin specifically how?

Mr. STAVRIDIS. Two ways. By attacking his accounts and diminishing them or by simply revealing them to his people. You are currently seeing Prime Minister Medvedev under enormous political pressure in Russia, a whole series of demonstrations around the country tied to revelations about his offshore financing, his yachts, his multiple luxury goods. That kind of reveal I think would have a salutary effect.

Senator WICKER. General Hayden, are you wanting to jump in there?

Mr. HAYDEN. Yes, just very briefly. Jim wrote about this right after the attacks became public, and one of the other ideas I think that was contained in his original article is so you have the Russians attacking the foundations of American democracy. So we return the favor. We use cyber tools to attack the foundations of Russian autocracy, which is the ability of the Russian surveillance state to track its own citizens. So pushing in a covert way tools into the Russian cyberspace that make it more difficult, anonymizing tools to make it more difficult for their security services to follow their own citizens demonstrates the cost to Putin of his fooling with our processes.

Senator WICKER. General Clapper, what might the counter-response be?

Mr. CLAPPER. Well, you preempted me, Senator. I am all for doing this, but there needs to be also due consideration for what the potential counter-retaliation might be. Of course, while we think in terms of very specific attacks, Putin's bank account or the oligarchs' around him, they may not react in kind. That is not to say not to do it. It is just that we need to consider what the potential domain or expanse of—what the space would be that they might retaliate against us. Ergo, my point about resilience.

Senator WICKER. For instance, how might they?

Mr. CLAPPER. Well, they could go after our critical infrastructure, for example, unrelated to the fairly narrow attack we might mount using Admiral Stavridis' example. That is not to say that, well, let us go after President Trump's bank account or something. That would be pretty big. It may not be a good example. But anyway, we cannot——

Senator WICKER. Or General Clapper's bank account.

Mr. CLAPPER. Well, that will be trivial.

All I am trying to say is we cannot count on an equal or symmetrical counter-retaliation if we retaliate. That is not to say we should not think about it and consider it. All I am asking or plug-

ging for is that we also consider about what the total space might be for a response.

Senator WICKER. General Clapper, you felt that the response in the example of North Korea was unsatisfactory. What might we have done other than sanctions, which you viewed as ceremonial, that might actually have helped the situation?

Mr. CLAPPER. Our leverage, U.S. direct leverage, over North Korea is kind of limited. You know, we are pretty much out of Schlitz on direct binary sanctions. Of course, what we have tried to do is to influence the Chinese, who do have some leverage over the North Koreans. What we wanted to do, of course, was to counter-attack. We knew what it was because it was attributed exactly. But then you run into the complication of you have to go through another country's infrastructure to get to the target. We were inhibited from doing that primarily from the standpoint of—again, this gets back to the definition of what is an act of war. Would that have been an act of war against a third country?

Senator WICKER. Quickly. We have talked about state actors and then non-state actors. How expensive is it to be in this business, if you are a non-state actor?

Mr. CLAPPER. How expensive is it?

Senator WICKER. Yes.

Mr. CLAPPER. Not very. Not very. If you want to roam around the dark Web and acquire tools and capabilities, it is not all that expensive.

Senator WICKER. So how expensive would it be for our government to gear up significantly in this regard?

Mr. CLAPPER. To gear up for an attack?

Senator WICKER. Well, to be more of a major player and to get organized and do what has been recommended at this table.

Mr. CLAPPER. Well, I do not know. I cannot answer the question, how much it would cost. I just would again foot stomp. I am sorry to sound like a broken record, but to me I do not think it is within the realm of possibility to completely foreclose a counter-attack. If we attack, we are going to be counter-attacked I would guess, and we need to be prepared for that eventuality. I guess what it does say, if we have money to invest, we need to think about defense first before we get off on all of the offensive tools which we are going to be inhibited from using unless we are confident in our resilience.

Senator WICKER. Thank you, gentlemen.

Chairman MCCAIN. Senator Shaheen?

Senator SHAHEEN. Thank you, Mr. Chairman.

Thank you all very much for being here.

I just want to follow up a little bit on the whole issue of sanctions because, as you said, General Clapper, you felt the sanctions against North Korea were not very satisfying. That is kind of how I felt about the sanctions that we did against Russia after the elections. They were not very satisfying.

On the other hand, there is a much more comprehensive sanctions bill that is sponsored by Senator McCain and has bipartisan cosponsors that would go after the energy sector, for example, and some of the financing in Russia. Do you think that would be a better way to hold Russia accountable for what they did?

Mr. CLAPPER. Well, it would certainly convey a message to them, no question about it. But again, what will they do in response? I am all for sanctions——

Senator SHAHEEN. Well, it is not a cyber response.

Mr. CLAPPER. The sanctions that we have imposed particularly after Ukraine were effective. They probably lowered the GDP [Gross Domestic Product] of Russia 2 or 3 percent. But, of course, the major problem Russia has is the price of oil going up and down. That is really what affects them.

But I think we could do and could have done more targeted sanctioning against certain figures in Russia. I do think kicking out 35 intelligence operatives and closing the two dachas was a great first step.

Senator SHAHEEN. I agree.

Mr. CLAPPER. But I would have like to have seen more.

Senator SHAHEEN. But I understood you all to say that if we do not take action in response to what has happened, whether it is Russia or North Korea, that we will continue to see these kinds of intrusions.

Mr. CLAPPER. Absolutely. That has been the pattern. You know, there has been an insidious increase. As adversaries, whether a nation state or a non-nation state, they are encouraged to push the envelope, and how much can we get away with? If there is no reaction, they will keep pushing that envelope.

Mr. STAVRIDIS. I will just add a way to think about this is the old saying if you live in a glass house, you should not throw stones. I do not agree with that in this case. We do live in a glass house. I think we need to throw a few stones, or we are going to see more and more of this and it will ratchet up over time.

As to the point about being unable to go after somebody because it goes through another nation's server setup, I take the point. I would counter by saying we fly Tomahawk missiles over other countries' airspace pretty consistently when we want to go after a target. So while I understand the legality piece of that, I think tactically that is not an insurmountable barrier.

Mr. CLAPPER. We do not do that over China or Russia.

Mr. HAYDEN. That was one of the issues I was suggesting of what down here applies up here. So I can offer just an hypothesis. Does a server in Malaysia enjoy as much Malaysian sovereignty as the building it which that server is located? The fact of the matter is I have seen very good legal minds take that on, and the answer is, no, it does not because it exists up here. In addition to its physical location, it also exists up here in this global commons, as if it were in space or at sea.

Senator SHAHEEN. Well, I think it is no doubt that our legal framework has not caught up with our technological framework.

I would go to your point, Admiral Stavridis, about education. I think one of the challenges is that this a topic that is so foreign to so many people that they do not have any idea how to address it. I mean, witness the audience at the hearing today. I think that is an example of that.

One of the things that struck me reading about the hack into Macron and the French elections was how simple the response of the Macron campaign was to what Russia was doing. They only

had 15 people, and what they figured out was if they put out a lot of decoys basically with a lot of information, that it would really blunt that attack. I think part of our education effort needs to be to explain to people that this is not as complicated as it seems and in terms of personal security hygiene.

But could government, knowing that the aversion to regulation that we have—would it not be possible for us to require any system that could be hacked that is sold to the government to have certain security requirements that would make it difficult to hack? Is that an option that we should be thinking about?

Mr. HAYDEN. Absolutely, ma'am. What that does because the government is such a big consumer, the water level of security in the country then goes up.

Mr. CLAPPER. To be religious about somehow mandating staying up with patches. Whenever there are changes, make sure that those are updated and somehow making that mandatory.

Senator SHAHEEN. Let me just ask a final question, if I could, Mr. Chairman, and that is, what is the current or potential cyber threat to this country that you all are most concerned about?

Mr. HAYDEN. I will jump in first. There is always a possibility of the apocalyptic attack, turning out all the lights east of the Mississippi. That is not where I focus. I cannot say that is zero. So, ma'am, if I draw a chart here in the ether between us as to how bad could it be, Hayden, and this arm is, yeah, but how likely is it, where I end up with is kind of Sony North America plus what the North Koreans did against Sony North America, perhaps enriched by new technology and more aggressiveness in the 2 years. So that is kind of my circle as most likely, most dangerous right now, which if done in sequence over multiple firms, I mean, that is a foreign government attacking a North American firm to coerce its behavior. Wow.

Mr. STAVRIDIS. I am just going to add to that. Even though I agree completely with the General that the likelihood is low, I think the grid is very vulnerable. I think that is worth spending more time to my other General's point about resilience because that is really the dark end of the spectrum, as General Hayden says.

Mr. CLAPPER. I think your question was most likely. I worry about the worst case, which is an attack on our infrastructure. I think the Russians particularly have reconnoitered it and probably at a time of their choosing, which I do not think right now is likely, but I think if they wanted to, they could do great harm.

Senator SHAHEEN. Thank you all very much.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Fischer?

Senator FISCHER. Thank you, Mr. Chairman.

Thank you, gentlemen, for being here today.

As the chairman said at the beginning of this hearing, many of us on this committee have talked for years about the need for a strategy and policy and a definition of terms basically. I think, Admiral, we continue to struggle in defining some key terms when it comes to cybersecurity. In your statement, you mentioned establishing a solid doctrinal foundation, a common vernacular for cybersecurity policy throughout our government.

General Hayden, you spoke about we have the opportunity before us right now where we can establish some case law internationally, a normative regime.

On an international stage, what are the consequences for our reluctance to move forward in establishing those terms, and how do you view the leadership of the United States in this process? I would ask you all to comment on that please.

Mr. HAYDEN. We suffer from a lack of internal consensus, and therefore it is hard for us to begin to build outward from that. If you are asking so if we were to go do that, how would we do that, my instincts are you begin within the Five Eyes community, likeminded English speaking democracies. You develop a consensus there, build out to maybe the G–7 countries who have real skin in the game in terms of cybersecurity, and then maybe out to the G–20. If you get broad normative consensus, not treaty consensus, in those groupings, then I think you have established international norms.

Keith Alexander, my successor at Fort Meade, had a wonderful question to a group once. Is there anyone in this room who knows a redeeming social value for a botnet? Of course, the answer is no. I mean, we can establish normative behavior that if you have a botnet on your network, it is kind of like you have biological weapons. There is no good reason for you to allow that to continue. Again, it requires consensus on our part and building out from that consensus to likeminded nations.

Mr. STAVRIDIS. I agree with all that. I will add to it. Over time when you really want to build that out, there is kind of a rough analogy, Senator, to what we did in the oceans in the creation of the Law of the Sea. You will recall before the 1980s, some nations had 200-mile territorial seas. Others had 3 nautical miles. Crazy claims were coming into place. The international community came together and created a Convention on the Law of the Sea. There is long back story about U.S. involvement there that we will not go into at this hearing. But the point is the international community eventually is going to grapple with this in some form or another.

The botnets are like pirates at sea. Nobody wants them. There are real demand signals emerging for more organization. We do not want to outsource this to the United Nations. We do want to build it from the inside out.

Senator FISCHER. So you agree with General Hayden when he said it is up to us, that we have to establish it first.

Mr. STAVRIDIS. Emphatically.

Senator FISCHER. Before you speak, General Clapper, in the NDAA [National Defense Authorization Act] we have included some things on cyber mostly to train, equip a force. But do you think this burden lies on us here in Congress, or does it take leadership from an administration willing to step up?

Mr. STAVRIDIS. I take the easy way out. It is both. You have to have a driver at the other end of Pennsylvania Avenue, but you have a role, obviously, in the ultimate disposition, as well as at times driving the other end.

Senator FISCHER. And defining it? Thank you.

General Clapper?

Mr. CLAPPER. I was just going to strongly endorse the Air Force guy, but I think the Law of the Sea is a great metaphor. I would also point out that took years and years, decades, hundreds of years to evolve. But there is a pretty sophisticated set of laws that seafaring nations generally abide by, and I think that is not a bad basis for thinking about the cyber domain.

So could we prevail upon countries to not attack civilian targets, for example, which would be to everyone's mutual advantage?

I think the United States must take the leadership here if for no other reason than the dominance of the United States in the technology and as much of the world's infrastructure that originates here or passes through this country. The obvious international leader here has got to be the United States.

Senator FISCHER. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator King?

Senator KING. Thank you, Mr. Chair.

First, I want to say this is one of the most informative and interesting and important hearings that I have attended in this or any other committee. I want to thank all three of you. It has been very provocative.

On Senator Wicker's question about cost, remember he was saying what it will cost. Just a rough calculation, for the cost of one jet aircraft, the Russians can hire 4,000 hackers. I mean, what the Russians did in our elections was warfare on the cheap. I mean, it was very low cost and very disruptive. I think that is part of the new reality that we are facing here.

I think Senator McCain asked a relevant question. We keep talking about a policy and a doctrine, and it never seems to happen. In my view, the major impediment is the structure which is so cumbersome and confusing and overlapping and dispersed that that produces cumbersome, overlapping, and dispersed policy. Structure is policy in my experience.

I think this really has to start with the only centralized authority we have in this country and that is the President. It has got to start with the direction from the President that we are going to have a policy. We are going to call together the intelligence community, the defense community, Homeland Security, and we are going to develop a policy and a doctrine.

I think the other piece that is very important that you have talked about is digital literacy. I think it needs to start in the third grade. Every American child at some point in their youth starts carrying around a computer, and they have got to be educated. In Maine, we have a very extensive—computers in our schools. Every middle school student in Maine has a laptop—every seventh and eighth grader in the whole state. We call it digital literacy, digital citizenship. People need to understand how to block their doors.

I was really struck, Admiral, by your statement that 65 or 70 percent of the attacks are essentially preventable. That is really a huge—our education has not caught up with it. We teach kids how to do things in day-to-day life, but we got to teach them how to distinguish truth from fiction on the Internet. My wife has a sign in our kitchen that says, "the problem with quotes on the Internet is

it is difficult to determine if they are authentic,"—Abraham Lincoln. We have got to be teaching those things.

Deterrence. I completely agree. We are all aging ourselves, but the relevant case to me is Dr. Strangelove. If you have the ultimate deterrent device but do not tell anybody, it is not deterrence. It does not work. Dmitri, why did you not tell us? Well, we were going to wait until May Day or something like that.

Then finally, there is a question in here somewhere. General Hayden, I think we have really got to be thinking hard about how we integrate with the private sector. Around here we always talk about whole-of-government. This has to be whole-of-society. The business community is very suspicious of government. They are worried about regulation. They do not want the Federal Government telling them what they got to do in their networks.

Give me some thoughts about how we can bridge that gap because if we do not, it is the private sector, it is the grid, the financial system. That is where the bombs are going to fall, in effect. That is why there has got to be more communication and cooperation, it seems to me, or it is just not going to work.

Mr. HAYDEN. Two very quick thoughts, Senator.

One, back to Senator Reed's comment about insurance. That is a far more attractive approach to the business community for the government to assist, support, unleash business to have better security through a return-on-investment model. That is one.

Second, back to my hand puppet here, all of our cultural habits in the executive branch and in the Congress are that the government has primary responsibility, the government is in the lead in terms of providing safety in physical space. Therefore, the private sector is always subordinated to the government. That is our habit of thought. The government tells the private sector what it is it has to do. That may not actually be a suitable model for this. This is a place where the private sector might actually have a larger chunk of the responsibility for security——

Senator KING. In my experience, the private sector overestimates their invulnerability. If you ask any utility in the country, they will tell you we have got it covered. We are okay.

Mr. HAYDEN. Perhaps because I am consulting with them and they want help, I see a different picture that they do recognize the issue.

For example, we talk about classification. We just got to get better at metering out formally classified information to the private sector. Yes, I get that. But you realize that is embracing the old model where the government is in control of what information is shared. I think, given enough time, I can think of seven or eight examples where it is not about making the old model, government is on lead, but we will cooperate more with you, work better. But perhaps changing the paradigm that in all but the most extreme cases, we are going to win or lose a cyber engagement based upon the private sector's performance. So now it is about liberating, unleashing, removing liability, and a whole bunch of other things that would make the private sector more self-reliant and frankly probably a better partner with the government.

Senator KING. I think one thing that the government can do—and General Clapper mentioned this in his agency—is red teaming

the dickens out of this, in other words, trying to break in and showing people where the problems are, whether it is within government or within the private sector.

Mr. CLAPPER. Two other points just to reinforce what Mike just said is, first of all, the private sector could well be the first line, you know, the DEW [Distant Early Warning] line, to use a Cold War—a distant early warning line could come from the private sector that would know about an attack, particularly the beginning phases, before the government might.

The other thing is the government cannot fully understand what is really important to the private sector segments. There has just got to be a better dialogue.

Now, having said that, I have to plug the Department of Homeland Security because I do believe it should be the interface with the private sector, not the spy community directly. We need to support that, but there needs to be that buffer because there is concern, sensitivity, maybe some of it well justified, about the spy crowd doing that. But there needs to be a more robust partnership between what the government, which cannot necessarily dominate this—and I completely agree with what Mike said, that the paradigm here may be different.

Senator KING. Thank you.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Rounds?

Senator ROUNDS. Thank you, Mr. Chairman.

Gentlemen, first of all, let me begin just by saying thank you very much for your service to our country.

I am just curious. If we had it to do over again and you could start right from 20 years ago and you were going to establish how we affected this domain, would you share with me, if you could begin at that time, what you would look at in terms of how we would establish this today? Where would we be today?

Mr. HAYDEN. So I had something of this question when I got to NSA. That is 1999. I thought I was being overly dramatic by going to the private sector to do our IT system. So we actually went to the phones, the computers, the network that for me by 2001 was actually being run by the private sector. My thought was that is good. That is an appropriate role. It would be inappropriate to more deeply involve the private sector in the mission aspects of what it was we did at NSA.

I may have low balled that. That may have been a bad judgment. In other words, as we are breaking new trail here—I began this more than 20 years ago. So in the mid-1990s, we probably should have more aggressively pushed not to extract private sector technology—we did that all the time—but to engage the private sector, particularly in the defensive aspect of this, out of the gate, that this is going to be won or lost based on their performance.

Mr. STAVRIDIS. I would add I take General Clapper's point. I think we would probably have centralized this in one entity. DHS did not exist then, but let us hypothesize that it did. I think you would probably start off with a more centralized function in the government. I like General Hayden's points on private/public.

As I mentioned in my initial thoughts, I would certainly consider building some kind of a cyber corps, a cyber service, a cyber first

responder force. I would also add look at the very beginning at the international aspects of this. We are flying that airplane and trying to do significant reconstruction on it. If we could get the international community together. I think there are lessons in all of those for today as well, Senator.

Mr. CLAPPER. Well, let me contradict what I said in my statement about if we could go back 20 years plus and start with a blank piece of paper, I think the notion of a cyber guard service, patterned somewhat after the Coast Guard—I am not even sure it needs to be a uniformed or could be a uniformed service. It may be better if it were not. I do not know. But that notion I think does have functional merit, and it would have been a lot easier had we grown that from the get-go when all of this started. But as always, hindsight is 20/20.

Mr. HAYDEN. Can I just add to that, Senator, very quickly? This is my talking about myself because I did this.

We can be fairly accused of militarizing the cyber domain. It was our armed forces that went there first. As I said, it is a domain of operations rather than this global commons. What Jim just suggested if we had been smart enough in the 1990s to have begun this with the Coast Guard-ish model, we may actually be in a better place globally than we were by using the Department of Defense model.

Mr. STAVRIDIS. A lot of this is how you think about it. So General Hayden has been using his hand puppet all morning. I agree with that.

I think another way to think about it is like an iceberg. The tip of the iceberg is really what the government can do. The mass of the iceberg here is really the private sector. If you hold that image in your mind 20 years ago, you would be in a very different place today.

Mr. CLAPPER. 85 percent of the critical infrastructure in the United States is in the private sector.

Senator ROUNDS. The Defense Science Board made it pretty clear that over the next 10 years, we are going to have to be able to deter those near-peer competitors because regardless of how hard we try, we can make it more expensive for them to get in. But we are not going to be able to necessarily stop them. Our defensive capabilities simply will not meet their offensive capabilities. There has to be a significant price to be paid for getting in. Agree or disagree?

Mr. CLAPPER. For me, listening to what you just said, again, I am being a broken record here, but it emphasizes the importance of resilience in my mind.

Mr. HAYDEN. I would just add do not confine your concept of defense as reducing vulnerabilities or defending at the perimeter. The best minds in this now in the private sector—it is presumption of breach. They are getting in. Get over it. Fight the fight. It is about discovery, recovery, response, resilience, not about the preventing penetration.

Mr. STAVRIDIS. If we can shift analogies yet again, think about it medically. If you go into a place with Ebola, today we go in with moon suits to try and protect our perimeter. The fight of the 21st century is inside the body. It is antibiotics. It is finding the

immunotherapy. It is knowing that you are going to be infected. How are you going to deal with it medically in the aftermath?

Senator ROUNDS. Thank you. My time has expired.

Thank you, Mr. Chairman.

Chairman MCCAIN. Senator Peters?

Senator PETERS. Thank you, Mr. Chairman.

Thank you, gentlemen, for very insightful testimony as always. I always appreciate your comments.

I will just, before I ask a couple questions, pick up on a comment. Admiral, you mentioned the 65 and 70 percent of attacks with proper hygiene. As you were saying that, it reminded me of a recent trip I had to Microsoft with their cyber folks there and a statistic that was my main takeaway from it was that they said that if you buy a computer at your local store and plug it into the Internet and you do not put any kind of software protections against viruses, that that computer will be infected within 17 minutes, which is pretty frightening and should be a real clarion call to everyone why this hygiene is so important. In 17 minutes. Just doing your normal Internet stuff, in 17 minutes it will be infected. That is the magnitude of the threat that we face particularly in the civilian side as you mentioned.

I want to continue to follow that line of thought because I think that is my major takeaway from this meeting as well. When you were asked, all three of you, the number one threat, each of those were in the civilian sector. They were critical infrastructure. It was the Sony attack. It was the grid. It was infrastructure generally.

You also talked about the silos and the concerns. I know, General Clapper, you talked about concerns of silos if we have a different command as well.

But I also appreciate your comments about how the Department of Homeland Security needs to be intricately involved in this whole aspect.

So my question is, given the dual nature of how we deal with this threat with the FBI and Homeland Security, Department of Defense, what do we need to do to bring that collaboration together? Is that perhaps part of this new cyber command, however it may be constituted, to involve kind of a real paradigm shift when it comes to different agencies that have these different kinds of responsibilities? Would the FBI be part of it, for example? Or what are your thoughts about what that would look like to incorporate some of our homeland security elements? To all three of you actually.

Mr. CLAPPER. Well, let me start. I guess I am the most recent graduate of the government. That is something actually we worked at pretty hard trying to graphically portray what the respective responsibilities are. I mean, the FBI, for example, hugely important. Of course, it all starts with attribution because then that determines the government response.

So if it is a criminal hacktivist that is in the United States, the first question, where is this coming from. Is it coming from overseas? Is it coming from a nation state? Is it coming from a nonnation state entity overseas, or is it coming domestically? The way we are currently organized and the way our laws govern us, there is a division of effort here among those players.

That is why the Department of Homeland Security I think is actually a very prominent player both for interface with the civilian sector and for resilience, you know, being the cyber FEMA [Federal Emergency Management Agency], if you will. When we have an attack—it is inevitable we are going to have them, and if it is of a sufficient magnitude, we have to have a mechanism for resilience, for recovery.

I do think—that is why I alluded to this in my remarks—that the setup we have today can be made to work provided people have the authorities that are supported by the Congress and the resources to discharge their respective responsibilities.

Mr. STAVRIDIS. I agree with that.

Mr. HAYDEN. All true.

A couple of additional thoughts. Number one, you got to man up. The Department of Homeland Security is notorious for having vacancies in senior leadership positions, particularly in the cyber aspects of it. So good talent there for extended periods of time.

Second I think is to end any sense of competition between Homeland Security and NSA, to have Homeland Security and NSA totally agree that NSA can be the powerful back room, but the storefront always has to be the Department.

Senator PETERS. One follow-up, if I may, and I am running out of time. I think, General Hayden, you mentioned about the civilian sector is very engaged in this, and I agree. I am very involved in the area of self-driving vehicles coming from Michigan. This is transformative technology. Certainly they are very aware and are focused on cybersecurity in that area. It is bad enough when someone breaks into your bank account, steals your money. If they take over your automobile, that is an existential threat to you—and have formed ISACs [Information Sharing and Analysis Center] and other ways to cooperate.

So your assessment of what you are seeing in the civilian sector with ISACs and other types of ideas that they are coming up with. What is your assessment of their effectiveness and how that might be able to be incorporated in this type of reorganization we are thinking about?

Mr. HAYDEN. No. They are a good news story, but they are uneven. Across different industries, you get different degrees of commitment, largely based on sense of threat. I actually think that the power industry, financial services—they are ahead of the pack because they know the dangers out there. It is not surprising that you are seeing that kind of cooperation here. But that would be the word "uneven" today.

Mr. STAVRIDIS. I will give you one good one specifically is the banking sector. The eight largest banks in the United States have come together to form something called the FSARC [Financial Systemic Analysis & Resilience Center]. I will send something in for the record on that.

Mr. STAVRIDIS. But it is a good news story. Again, it goes to General Hayden's point about a sense of threat. They ought to feel threatened and they are working together to alleviate that threat.

Mr. CLAPPER. I would just endorse that. The financial sector in this country has gotten religion about this for obvious reasons. That is a great model for this.

Senator PETERS. Thank you.

Chairman MCCAIN. Senator Nelson?

Senator NELSON. Thank you, Mr. Chairman.

Gentlemen, thank you for your public service.

I get the impression from your testimony that we really have not responded in any way to give the deterrence that we want. So let us take a couple of examples: the intrusion into our election and now the French election and we expect the German election. Give me a scenario that you might think that we might respond so that anytime that the Russians are fooling around in the future in Ukraine, Syria, other elections, what would be a good deterrence.

Mr. CLAPPER. Senator Nelson, I spoke briefly to this at my earlier hearing before Senator Graham's Judiciary Subcommittee. I think frankly—and I mentioned then, as much as I do not like doing hearings, that I thought it was a useful service for the public to have this discussion about the Russian interference, which in my mind far transcends leaks and unmaskings and all that. That is all internal stuff. But this assault on our democracy by the Russians I think is profound. The public has got to be educated and it starts with education, just as we were talking about with cyber.

So I will again contradict myself about how the government is organized with respect to messaging or counter-messaging. I would vote for a USIA, a United States Information Agency, on steroids to do the counter-messaging for election interference or counter-message ISIS [Islamic State of Iraq and Syria] or any other message that is inimical to our interests and our values because our messaging right now is fragmented across the government. I have said this before, and the experience we had with this egregious interference in the most important process of our future of our democratic system has got to start with educating our public and doing the counter-messaging against those nefarious messages and the sources of them.

I do think the French went to school on our experience. In the course of developing our intelligence community assessment, we shared with our friends and allies what we were experiencing. But that to me is a fundamental shortfall in the way we are organized now.

Senator NELSON. Let us hope the Germans do as well.

Mr. HAYDEN. Senator, I would do all that as part of a component of a broader response. Here, I would drop what you described not in the information warfare box or in the cyber box. I would drop this in the "we got a problem with the Russians" box. I would respond across the board.

So in response to this, I would sell arms. I would give arms to the Ukrainians. I would do everything that Jim described in terms of cyber counterpunching. I think I would have the President fly up to Erie, get in a motorcade, stand on top of Marcellus shale and say this is going to Europe. This gas is going to wean our European friends off their dependence on Russian energy, and we are going to do that in 10 years.

Senator NELSON. I happen to agree. I think we ought to make a bold display of our displeasure. Let us hope that because of our misfortune in our election that, again, it is arming the Germans,

as it apparently has armed the French. Part of that was an education campaign, just what you said, General.

All right. So the private sector, though. So, you know, they are really dragging their feet. We have not been able to get them to quickly share threat information with the government, and incentives are not working at the level that we need. So how do we need to change that private sector's thinking?

Mr. HAYDEN. Very briefly. Number one, keep on doing what we are doing. Keep pressing ahead. Make ourselves a more welcoming and more generous partner in the dialogue, again, back to the paradigm where we are in charge of what is getting shared and they get whatever we decide, again, probably not the right model, far more cooperative.

Mr. STAVRIDIS. I would just add specifically the cyber insurance piece that we have talked about—that is a very practical piece of this. Doing a hearing like this—you probably are—with Eric Schmidt of Google, Dan Schulman of PayPal, Bill Gates of Microsoft, get those voices. You are probably already doing that.

Mr. CLAPPER. I do want to mention, Senator Nelson, the pushback that Jeh Johnson, then Secretary of Homeland Security, got from state election officials when he attempted to engage with them particularly on the issue of including our voting apparatus at large as part of our critical infrastructure. So there is a lot of suspicion, whatever it is, pushback at the state level and local level about the Feds getting involved in things, just another manifestation of this reluctance on the part of the private sector to engage.

Mr. STAVRIDIS. Can I just pick up the last point about the states? We have not talked enough about the States and their role in all of this. I am joined today by Dave Weinstein, who is the head of cyber for the State of New Jersey. They have a hub and spoke relationship with the Federal Government. We need more of that to break down those stovepipes in this area like we try to do in law enforcement.

Senator NELSON. Amen. Thank you.

Chairman MCCAIN. Senator Blumenthal?

Senator BLUMENTHAL. Thank you, Mr. Chairman. Thank you for having this hearing.

This hearing illustrates for me one of the ironies of working here, which is that we are discussing one of the most important topics to our national defense with one of the most erudite, informative panels in my experience on this committee, and the room is empty.

Mr. STAVRIDIS. Hopefully, we are online somewhere.

Senator BLUMENTHAL. I am sure we are online somewhere, but it really illustrates I think the point that each of you has made about education and the focus that needs to be devoted to this topic. I was reminded—I do not know why exactly—as one of you was testifying of a book called "Why England Slept," now a famous book because it is written by a former President, John F. Kennedy, about England's sleeping through the buildup in Germany and that buildup left it very far behind when it was directly and immediately threatened. I feel we are living through the same kind of era right now in cyber, and we will be, I fear, tragically awakened to our complacency at some point.

General Clapper, you said in that Judiciary hearing—and you were very powerful on this topic of the assault on our democracy—that there needs to be—and I am quoting—I do think as well there needs to be more done in the way of sanctions to the Russians or any other government that attempts to interfere with our election process. End quote.

I have cosponsored and helped to introduce two measures, Countering Russian Hostilities Act and Russia Sanctions Review Act, that seek to codify and impose greater sanctions on the Russians. I believe, as Senator Graham said at that hearing and both of us have said recently, that the Russians will continue to attack us—2018 is not very far away—as long as they are not made to pay a price or, as the chairman said, as long as the benefits outweigh the price that they pay. That is just the calculus for them, and they are going to continue to do it.

But I also think that people who cooperate with them, aid and abet, collude also should be made to pay a price when they violate our laws. There is an ongoing investigation conducted by the FBI into not only the Russian interference with our election but also potential cooperation or collusion they receive from Americans, including members of the Trump campaign, Trump associates. Michael Flynn is subject to that investigation.

Assuming that all of you agree that anybody in this country who cooperates or colludes with that kind of cyber attack, which I regard as an act of war on this country, I am wondering whether I could elicit from you support for appointment of a special prosecutor? I realize it may be somewhat outside the sphere directly of the technical issues that bring you here today, but I do think it is of paramount importance. You raised this issue by referring to domestic threats in the cyber sphere, General Clapper. You were on CNN [Cable News Network] this morning, General Hayden, talking about this topic exactly about your previous opposition to such special prosecutors but now perhaps you have a somewhat changed view because of the events of the last 48 hours and the need for what you called, quote, extraordinary structure to uncover the truth and impose accountability.

So with that longwinded buildup—and I apologize for being so longwinded—let me ask you, General Clapper and the rest of the panel, maybe beginning with General Hayden.

Mr. HAYDEN. I will go first because you are quoting me from a couple of hours ago in which I said I instinctively oppose—these sorts of extraordinary structures go longer, deeper, broader than you want and they become destructive in their own right. But I have been disheartened by the events of the last 48 to 72 hours. I am not yet decided, Senator, as I said on CNN, but I am very close to having—I have a far more open mind than I did before lunch 2 days ago, and we will see now whether the ordinary structures can give the Nation sufficient confidence that they will not be impeded, they will be enthused, and they will get to the truth and be able to tell us the truth.

Mr. CLAPPER. I worry about multiple investigations in the Congress, which I think have the effect of dissipating energy. As a frequent witness to these many investigations, I am in the same place

that Mike is where I have reached the point where I believe that we need to think about that.

I have previously spoken in hearings that I thought probably the best hope in the Congress was the Senate Intelligence Committee, but in light of the events of the last day or so, I am moving toward that pendulum swinging more towards some kind of independent effort. Whether it is a commission or a special prosecutor, I do not know.

What I do know is we have got to get rid of this cloud over this country. This is in the best interest of the President. It is in the best interest of the Republicans or Democrats. I do not care what the stripe is. But this is a profoundly serious thing for this country. We are in a bad place. I do not know what the solution is, whether it is some kind of independent body. Maybe that is where we need to go next.

Senator BLUMENTHAL. Admiral?

Mr. STAVRIDIS. I think this is beyond the scope of the executive branch. The events call for something outside the executive branch, much as an IG [inspector general] in the military sits outside a chain of command and can, therefore, effectively look. What that exact structure is I do not know, and I yield to the Congress to determine it. That is why we have a separation of powers in this Nation.

Senator BLUMENTHAL. I am way over my time, Mr. Chairman. I apologize.

Chairman MCCAIN. Well, it is an important question.

Senator BLUMENTHAL. Thank you.

Chairman MCCAIN. Could I just say to the witnesses this has been very important for this committee? We appreciate the gravity of the challenge, and you have certainly given us a lot of good advice and counsel.

Could I finally say that there are very few benefits of being around a long time that I know of.

We are about to adjourn, Senator Warren.

There are very few benefits, but one of them is the great honor that I have had to know the three witnesses over the years. I appreciate their wisdom, their counsel, and their outstanding service to our Nation. I know you had other things to do besides coming here this morning, but I am speaking for the entire committee. I am very grateful.

This hearing is adjourned.

[Whereupon, at 11:12 a.m., the committee was adjourned.]

○