March 2, 2017

# Cyber Strategy and Policy

Committee on Armed Services, United States Senate, One Hundred Fifteenth Congress, First Session

---

## Hearing Contents:

**Witnesses**

Keith B. Alexander
CEO and President
IronNet Cybersecurity
*View Testimony*

Craig I. Fields
Chairman
Defense Science Board
*View Testimony*

James N. Miller
Member - Defense Science Board
Former Under Secretary of Defense For Policy
*View Testimony*

Matthew C. Waxman
Liviu Librescu Professor of Law
Columbia University Law School
*View Testimony*

**Available Webcast(s)*:**

*Full Hearing*

**Compiled From*:**

*https://www.armed-services.senate.gov/hearings/17-03-02-cyber-strategy-and-policy*

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

*This hearing compilation was prepared by the Homeland Security Digital Library, Naval Postgraduate School, Center for Homeland Defense and Security.*

**Prepared Statement of GEN (Ret) Keith B. Alexander***
**on Cyber Strategy and Policy before the**
**Senate Armed Services Committee**

**March 2, 2017**

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. And 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.

* GEN (Ret) 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.

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."[1] 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 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."[2] 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.[3]

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

---

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

[2] *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> .

[3] *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.")

attack; [g]ather foreign threat intelligence and determine attribution; [and] [s]ecure national security and military systems."[4] Moreover, the "bubble chart," as this document was called, assigned the following lead roles: DOJ: investigation and enforcement; DHS: protection; and DOD: national defense.[5]

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.[6] 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,[7] and

---

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

[5] *See id*.

[6] *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.")

[7] *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-

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 (NCP$^3$).[8] 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."[9] Part of the NCP$^3$'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."[10] 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."[11] 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

---

partners/critical-infrastructure-and-key-resources> ("The private sector owns and operates an estimated 85% of infrastructure and resources critical to our Nation's physical and economic security.").

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

[9] *Id*. at 14-15.

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

[11] *Id*.

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 defense 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.[12] Moreover, while the government has placed this responsibility with DHS today,[13] 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.[14] 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.

---

[12] *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).

[13] *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.").

[14] *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.").

**Statement**

**By**

**Dr. Craig Fields**
**Chairman, Defense Science Board**

**And**

**Dr. Jim Miller**
**Member, Defense Science Board**
**Former Under Secretary of Defense (Policy)**

**Before the**

**Armed Services Committee, United States Senate**

# Cyber Deterrence

**March 2, 2017**

## 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?

*21st 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, **m*ajor powers (Russia and China)*** *have a significant and growing ability to hold U.S. 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 U.S. 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 defenses. 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 U.S. 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 U.S. 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.

# Cyber Strategy & Policy:
# International Law Dimensions

## Testimony Before the Senate Armed Services Committee

**Matthew C. Waxman**
Liviu Librescu Professor of Law, Columbia Law School
Co-Chair, Columbia Data Science Institute Cybersecurity Center

**March 2, 2017**

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]

---

[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/).

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 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

[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

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

---

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

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. 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

---

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.

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

---

[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.

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 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.

[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.