Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO
RECEIVE TESTIMONY ON
CYBER STRATEGY AND POLICY

Thursday, March 2, 2017

Washington, D.C.

ALDERSON COURT REPORTING
1155 CONNECTICUT AVENUE, N.W.
SUITE 200
WASHINGTON, D.C. 20036
(202) 289-2260
www.aldersonreporting.com

HEARING TO RECEIVE TESTIMONY ON

CYBER STRATEGY AND POLICY

Thursday, March 2, 2017

U.S. Senate

Committee on Armed Services

Washington, D.C.

The committee met, pursuant to notice, at 9:40 a.m. in Room SH-216, Hart Senate Office Building, Hon. John McCain, chairman of the committee, presiding.

Committee Members Present: Senators McCain [presiding], 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 HON. JOHN MCCAIN, U.S. SENATOR FROM ARIZONA

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 experience 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 HON. JACK REED, U.S. SENATOR FROM RHODE ISLAND

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 Command, 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 [RET.], 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. And 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 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:]

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. And 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. And then I'm going to turn it over to Jim and he's going to give you the main points, given time constraints, of our cyber deterrence task force. And then, of course, we'll enter into discussion later.

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

What is the DSB 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 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?

And 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 2, 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. And 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.

[The prepared statement of Dr. Fields follows:]

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.

And 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 U.S. 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 U.S. institutions which were intended to affect voter confidence and ultimately to affect the outcome of the recent U.S. 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 U.S. critical infrastructure at risk through cyber attack, and also a growing capability to hold at risk the U.S. military, and so to potentially undermine U.S. military responses. And 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. And 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 U.S. critical infrastructure. For this problem set, the U.S. 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.

And 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. And these capabilities need to be built out in a way that does not require burning intelligence axes when we exercise them.

And 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 U.S. strike systems. To credibly be able to impose unacceptable costs in response to cyber

attack by major powers, Russia and China, the U.S. 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 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 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, importantly, in the private sector as well, and to bring them to bear in a systematic way.

And 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.

And 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 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 prepared statement of Dr. Miller follows:]

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:]

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. And 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, 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? And second of all, what's the answer? What is the solution to what is clearly, it seems to me, a stovepiped scenario? And 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. And 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. And 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: And 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 JIATA, 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. And 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. And then we'll get the organizational structure that supports it.

Senator Reed: And 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. And 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: And, 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 '01 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.

And 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. And 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.

And 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. And 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. And 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 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? And 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. And 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 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. And 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. And 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, 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. And 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 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.

And 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. And 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. And 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 nine 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 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 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 policy 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 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 observing 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. And 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? And 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 seven 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. And 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 five 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. And 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. And 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, 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.

And 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. And 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. And 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, 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 U.S. 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: And 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. And 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 hearing was adjourned.]

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu