

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](http://www.aldersonreporting.com)

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

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.

1           OPENING STATEMENT OF HON. JOHN MCCAIN, U.S. SENATOR  
2 FROM ARIZONA

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

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

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

21          I have yet to find any serious person who believes we  
22 have a strategic advantage over our adversaries in  
23 cyberspace. In fact, many of our civilian and military  
24 leaders have explicitly warned the opposite. In short, this  
25 committee is well aware that bold action is required, and we

1 will continue to apply the appropriate pressure to ensure  
2 that the new administration develops a cyber strategy that  
3 represents a clean break from the past.

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

9       General Alexander recently served on the Presidential  
10 Commission on Enhancing National Cyber Security. Given his  
11 extensive experience as Director of the National Security  
12 Agency and the first commander of the United States Cyber  
13 Command, we welcome his insights and guidance as we seek to  
14 ensure that our policies, capabilities, and the organization  
15 of the Federal Government are commensurate with the cyber  
16 challenges we face.

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

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

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

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

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

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

13 Senator Reed?

14

15

16

17

18

19

20

21

22

23

24

25

1           STATEMENT OF HON. JACK REED, U.S. SENATOR FROM RHODE  
2 ISLAND

3           Senator Reed: Thank you very much, Mr. Chairman. I  
4 want to thank you for holding this very timely and  
5 incredibly important hearing.

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

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

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

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

1 Thank you.

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

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

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

1 critical issues and more.

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

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

16           The recommendation to develop a capability to conduct  
17 information operations is an important one. However, I  
18 would note that we currently have very limited capabilities  
19 for mounting effective information operations that are  
20 sought and called for in this report. The report calls for  
21 assigning this responsibility to Cyber Command, but the  
22 cyber mission forces were built for a different role. They  
23 were built for defending networks against intrusion and for  
24 penetrating and disrupting others' networks, but not for  
25 conceiving and conducting operations involving content or

1 cognitive manipulation.

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

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

11 Chairman McCain: Thank you.

12 As the members know, there's a vote that will begin at  
13 10 o'clock. Usually we just kind of keep the hearing going,  
14 but I feel that this hearing is so important that maybe  
15 we'll wait until there's about 5 minutes left in the vote,  
16 in the first vote, take a brief recess, and come back after  
17 the second vote. I just think that the issue wants us to  
18 hear the full testimony.

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

22

23

24

25

1           STATEMENT OF GENERAL KEITH B. ALEXANDER, USA [RET.],  
2           CEO AND PRESIDENT, IRONNET CYBERSECURITY

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

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

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

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

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

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

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

21 Over the last three months we've seen destructive  
22 attacks on Saudi Arabia by Iran, and we are not prepared as  
23 a nation to handle those. Our industry and government are  
24 not working together. My experience in the last three years  
25 of being a civilian is that industry does want to work with

1 government, but we haven't provided the relationships, and  
2 the roles and responsibilities of the different departments  
3 are not well understood. So I'll give you my insights of  
4 how those roles should be.

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

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

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

1           It's my opinion that the role and responsibility, as  
2 articulated in the Federal Roles and Responsibilities in  
3 Cyberspace, for defending this nation rests with the Defense  
4 Department. It's stated there. It's clearly to defend this  
5 country. And yet, when we talk to all of the departments  
6 about roles and responsibilities, it was clear that that was  
7 mixed up because we talked about different levels of roles  
8 and responsibilities, whether it was incident response, the  
9 role that DHS would have, by defending the nation.

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

14           I believe that in doing that, the technology exists.  
15 More importantly, it's been my experience that industry  
16 wants to work with government to help make this happen, and  
17 this is an opportunity for our government to stand together  
18 and do this.

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

1 of this nation, and we aren't doing that job.

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

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

10 Thank you very much, Mr. Chairman.

11 [The prepared statement of General Alexander follows:]

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 Chairman McCain: Thank you for your testimony.

2 Dr. Fields?

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

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

3           Dr. Fields: Good morning, Chairman McCain, Ranking  
4   Member Reed, members of the committee. And Jim, thank you  
5   for the microphone.

6           Dr. Miller: It's a technology issue.

7           Dr. Fields: It's a technology issue.

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

11          What I want to do is to start by giving you a little  
12   view of the landscape of the Defense Science Board's study  
13   on cyber more generally, because there are actually a lot of  
14   pieces of the puzzle, and then offer to you eight principles  
15   that cyber has to comply with if we're going to be  
16   effective. These principles do not dictate the details of  
17   what to do in any circumstance, but they're like laws of  
18   physics; you have to comply. And then I'm going to turn it  
19   over to Jim and he's going to give you the main points,  
20   given time constraints, of our cyber deterrence task force.  
21   And then, of course, we'll enter into discussion later.

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

24          What is the DSB going to do? Our study of cyber  
25   resilience, the main finding that's germane being that it's

1 simply not possible to defend against a high-level threat.  
2 We can defend against mid- and low-level threats, but the  
3 high-level threats, like we could have from China or Russia,  
4 we have to deter. That's not a statement of criticism of  
5 our capabilities. That's true basically of any country  
6 because the means of deterring of defense are just not up to  
7 the means of offense at this point in time.

8 Cyber and cloud computing. How can DOD take advantage  
9 of the benefits of cloud computing without the risks?

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

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

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

24 Acquisition of software. Parallel to a previous  
25 comment on micro-electronics, what we get is not always what

1 we expect to get. How can we mitigate the risk?

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

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

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

15 Part 2, fundamental principles. These are the eight  
16 principles that I think we should all pay attention to as we  
17 address the issue of cyber deterrence.

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

25 Number two and implied by the first, deterrence of an

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

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

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

23         Number five, and again implied above, is U.S. responses  
24 to cyber attacks do not have to impose only a similar level  
25 of cost on an adversary. It can be greater. We have to

1 obey the law. Mr. Waxman will address that, and I don't  
2 want to practice law without a license here. But we should  
3 be, again, flexible in our thinking even if we're prudent in  
4 our actions.

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

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

19       Seventh is chronology. It's a lot more effective to  
20 take deterring action quickly after something happens that  
21 you don't want to happen rather than waiting days, weeks,  
22 months, years. Chronology counts. That means you have to  
23 be prepared. The intelligence community has to collect the  
24 information in order to take action. CYBERCOM and other  
25 organizations have to be prepared to take action based on

1 and using that information. The executive branch has to be  
2 able to orchestrate if it goes across various departments.

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

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

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

20 [The prepared statement of Dr. Fields follows:]

21

22

23

24

25

1 Chairman McCain: Thank you.

2 Dr. Miller, welcome back.

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

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

4           Dr. Miller: Thank you, Chairman McCain, Ranking Member  
5   Reed, members of the committee. It is an honor to be here  
6   again.

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

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

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

24          In looking at the problem set, we found it useful to  
25   distinguish between three different sets of cyber

1 challenges. The first is that major powers, Russia and  
2 China specifically, have a significant and growing ability  
3 to hold U.S. critical infrastructure at risk through cyber  
4 attack, and also a growing capability to hold at risk the  
5 U.S. military, and so to potentially undermine U.S. military  
6 responses. And as Dr. Fields indicated, for at least the  
7 next decade the offensive cyber capabilities of these major  
8 powers are likely to far exceed the United States' ability  
9 to defend our critical infrastructure. And at the same  
10 time, the United States military has a critical dependence  
11 on information technology, and these actors are pursuing the  
12 capability through cyber to thwart our military responses.

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

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

1 actors.

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

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

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

1 Third --

2 Chairman McCain: Excuse me. I don't mean to  
3 interrupt. Your first point, we haven't done that.

4 Dr. Miller: That's correct, sir.

5 Chairman McCain: Okay.

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

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

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

22 The second broad category of recommendations was that  
23 the Defense Department develop what we described as a cyber  
24 resilient thin line of key U.S. strike systems. To credibly  
25 be able to impose unacceptable costs in response to cyber

1 attack by major powers, Russia and China, the U.S. needs key  
2 strike systems -- cyber, nuclear, and non-nuclear strike --  
3 to be able to function even after the most advanced cyber  
4 attack, and this is not a simple task. The task force made  
5 some specific recommendations and examples of long link  
6 strike systems to include -- that's included in the prepared  
7 statement.

8 In support of this thin line cyber secure force, the  
9 task force recommended three actions in particular. First,  
10 an independent strategic cyber security program housed at  
11 NSA to perform top-tier cyber red teaming on the thin line  
12 of cyber long-range strike and nuclear deterrence systems.  
13 The model is similar to what we have with the SSBN security  
14 program, which I know the committee is familiar with,  
15 looking at not just what could be done today but what could  
16 be done in future that has significant consequence.

17 A second component is a new best-of-breed cyber  
18 resilience program to identify the best security concepts in  
19 government and, importantly, in the private sector as well,  
20 and to bring them to bear in a systematic way.

21 And third, an annual assessment of the cyber resilience  
22 of the U.S. nuclear deterrent, similar to what's done  
23 currently for the nuclear deterrent more broadly. This  
24 would be conducted by the commander of the strategic  
25 command, and the certification would go to the Secretary of

1 Defense, to the President, and to the Congress.

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

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

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

16 And finally, and last but certainly not least, is  
17 sustained and enhanced recruitment, training, and retention  
18 of a top-notch cyber cadre.

19 At the end of the day, from all the importance of  
20 technology in this area, the most important strategic  
21 advantage of the United States in cyber, as in other  
22 domains, is the incredible capabilities of our military, of  
23 our civilians, and of our private sector. DOD has taken  
24 some important steps to move forward on recommendations of  
25 this report over the course of its conduct, in parallel with

1 its establishing its 133 cyber mission force teams. The  
2 recommendations which I've just described are intended to  
3 build on what the Department is doing to expand it and to  
4 accelerate it.

5 Again, thank you for the opportunity to testify today.

6 [The prepared statement of Dr. Miller follows:]

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 Chairman McCain: Thank you.

2 Mr. Waxman?

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

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

3           Mr. Waxman: Chairman McCain, Ranking Member Reed --

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

8           [Recess.]

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

13          Mr. Waxman: Thank you, Chairman McCain, Ranking Member  
14 Reed, committee members. I appreciate the opportunity to  
15 address some international law questions relevant to U.S.  
16 cyber strategy. These include when a cyber attack amounts  
17 to an act of war, as well as the international legal  
18 principle of sovereignty and how it could apply to cyber  
19 activities. I also have a written statement that I hope can  
20 be made part of the record.

21          These are important questions because they affect how  
22 the United States may defend itself and what kinds of cyber  
23 actions the United States may take. They're difficult  
24 questions because they involve applying longstanding  
25 international rules developed in some cases over centuries

1 to new and rapidly changing technologies and forms of  
2 warfare.

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

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

21 With those objectives in mind, I'll turn first to the  
22 question whether a cyber attack could amount to an act of  
23 war. When should a cyber attack be treated legally the same  
24 way we would, say, a ballistic missile attack versus an act  
25 of espionage, or should cyber attacks be treated altogether

1 differently with entirely new rules?

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

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

21 However, a cyber attack that crosses the force or armed  
22 attack threshold would trigger legally an even wider set of  
23 responsive options, notably including military force or  
24 cyber actions that would otherwise be prohibited. In recent  
25 years the United States Government has taken the public

1 position that some cyber attacks could cross the U.N.  
2 Charter's legal thresholds of force or armed attack. It is  
3 said that these determinations should consider many factors,  
4 including the nature and magnitude of injury to people and  
5 property.

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

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

21         However, the United States Government's approach to  
22 date leaves a lot of gray areas. It leaves open how to  
23 treat some cyber attacks that do not directly and  
24 immediately cause physical injuries or destruction but that  
25 still cause massive harm. Take, for instance, a major

1 outage of banking and financial services, or that weaken our  
2 defensive capabilities such as disrupting the functionality  
3 of military early warning systems. More clarity on this  
4 issue is important.

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

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

22         Now, as a policy matter, we have a strong interest in  
23 limiting infiltration and manipulation of our own digital  
24 systems, and it may usually be wise to seek consent from  
25 states that host digital systems that might be affected or

1 used in cyber operations. However, it is my view that there  
2 is not enough evidence of consistent and general practice  
3 among states, or a sense of binding legal obligation among  
4 them, to conclude that the principle of sovereignty would  
5 prohibit cyber operations just because, for example, some  
6 cyber activities take place within another state or even  
7 have some effects on its cyber infrastructure without  
8 consent, especially when the effects are minimal.

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

11 [The prepared statement of Mr. Waxman follows:]

12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

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

6 Mr. Waxman: Senator, I would call that --

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

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

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

19 Mr. Waxman: That's correct, Senator. I think there  
20 are certain categories of activity that can have tremendous  
21 effects on states' core interests. And at least  
22 traditionally, at least traditionally, international law has  
23 recognized only certain categories as justifying armed force  
24 in response.

25 Chairman McCain: Well, I thank you, but this is really

1 -- you raise several fundamental questions that have to be  
2 resolved by the Congress and the American people.

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

12       So, as I understand it, General Alexander and Dr.  
13 Fields and Dr. Miller, we have four agencies that are  
14 responsible against cyber attacks, the FBI, Homeland  
15 Security, Intelligence, and Department of Defense. They're  
16 the ones that are in the lead for defending the homeland,  
17 military computer networks, employing military cyber  
18 capabilities.

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

25       General Alexander: Chairman McCain, I agree, it's not

1 working. There are four stovepipes, and it doesn't make  
2 sense. If we were running this like a business, we'd put  
3 them together.

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

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

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

22 So what you have is people acting independently. With  
23 those schemes, we will never defend this country. And more  
24 importantly, when industry looks at our government, they  
25 are, quite frankly, dismayed. We are all over the map, and

1 no one can answer who is responsible. So you have to bring  
2 it together.

3 Chairman McCain: Are you sure industry is that  
4 interested in cooperating?

5 General Alexander: Absolutely. My experience --  
6 especially those who own critical infrastructure understand  
7 that they cannot defend that without government support.  
8 And working together, they see an opportunity.

9 Chairman McCain: Dr. Fields?

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

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

22 Is that a fair statement, Jim?

23 Dr. Miller: That's very fair.

24 Dr. Fields: So it is an unsolved problem. It's an  
25 unsolved problem because I actually think we do need a

1 campaign strategy to make this a continuous process. This  
2 is not inflation exercises. The exercises are in service of  
3 high performance in executing the campaign.

4 Chairman McCain: And we should start with a policy.

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

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

21 Dr. Miller, real quick.

22 Dr. Miller: Thank you, Chairman. I agree with your  
23 premise, and I agree with both General Alexander and Dr.  
24 Fields regarding the nature of the solution. I'm not  
25 convinced that a massive reorganization is appropriate,

1 certainly at this point in time, and I'd be looking toward  
2 an integrating body.

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

16 Chairman McCain: Thank you.

17 Senator Reed?

18 Senator Reed: Well, thank you very much, Mr. Chairman.

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

24 One of the things I share with General Alexander's  
25 concern is we're not really exercising with the commercial

1 world and the governmental world. We do it ad hoc. We have  
2 overlaps in logistics, but we have to know what some  
3 commercial companies can do, but then we have huge gulfs.  
4 Again, just quickly, your comments about how to act, because  
5 I think in terms of getting something done quickly, testing  
6 even a bad strategy or even an incoherent strategy but just  
7 going out to see where the holes are is better than,  
8 frankly, theorizing.

9 So, General Alexander, your comments. And then, Dr.  
10 Fields, I have a couple of other questions.

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

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

22 Senator Reed: And again, we're getting to the point of  
23 if it's voluntary, some people might come and some people  
24 might not. To be effective, it's going to have to be  
25 comprehensive, and there's going to have to be a certain

1 inducement, either an incentive or a disincentive.

2 Dr. Fields, your comments quickly.

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

11 Senator Reed: Dr. Miller, do you have a comment?

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

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

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

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

15           The fact that there is some unsettled gray area in the  
16 law here, on the one hand, makes it difficult to know where  
17 the boundaries are, but it's also an opportunity if we think  
18 about this strategically. We want the lawyers to be  
19 consulting with the policymakers on where they want to go  
20 and asking questions together, like what does a particular  
21 interpretation get us that we wouldn't otherwise be able to  
22 do; how might this limit us in other areas, let's say if  
23 we're engaging in offensive cyber operations; would this  
24 open the door to unintended consequences. So I think they  
25 need to be linked up.

1           Senator Reed: Just a final question. I have a couple  
2 of seconds left.

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

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

17          Senator Reed: [Presiding] On behalf of Chairman  
18 McCain, I recognize Senator Inhofe.

19          Senator Inhofe: Thank you. First of all, let me say  
20 to you, General Alexander, that it was back in '01 that we  
21 talked about involving the university. The University of  
22 Tulsa has become quite a leader in this area. Have you had  
23 a chance to see some of the progress since you left this  
24 job?

25          General Alexander: Yes. The last I saw, Senator, was

1 what they were doing in industrial control systems. I think  
2 that's really good, and I think the capabilities and the  
3 students they provide back to the government is great. So I  
4 do think pushing with universities education, just as you  
5 brought up, is something that we have to do.

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

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

15 Dr. Miller: Senator, I do.

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

20 General Alexander: I have the chart, and I'll tell you  
21 that first, when we talk to the different agencies, they  
22 don't understand their roles and responsibilities. So when  
23 you ask them who is defending what, you get a different  
24 response. So even though this is the Federal cyber security  
25 ops team, and this was put out by the White House to the

1 commission, when we asked the individuals, they couldn't do  
2 it.

3 The second part that you asked is, yes, I do think,  
4 Senator, that it needs to be brought together. That's the  
5 strategy we should put in place, how do we defend this  
6 country, and then let's walk through it, with the exercising  
7 continually evolving.

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

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

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

25 Dr. Miller: Senator, your comments make a lot of

1 sense. A common approach to engaging industry with  
2 information and a systematic effort to do that would be very  
3 valuable. I second General Alexander's earlier comments  
4 that in my experience sometimes industry is unsure with whom  
5 to engage, and the people on the government side are  
6 sometimes unsure who has that responsibility as well.

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

14 Senator Inhofe: I agree, and I appreciate that.

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

19 General Alexander: Will do, Senator.

20 Senator Inhofe: Okay. One thing, one issue, and you  
21 brought this up, Dr. Miller, in your statement you said,  
22 "the declaratory policy that makes clear the United States  
23 will respond to all cyber attacks. The question will not be  
24 whether but how." Of course, you brought up something, Dr.  
25 Fields. In your eighth point you said, "Credibility is a

1 necessary enabler of deterrence. If a leader we want to  
2 deter does not believe we will act, it is difficult to  
3 deter. Announcing red lines and then overlooking offenses  
4 is not constructive.”

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

7 Dr. Fields: You reestablish credibility not by making  
8 a declaration alone but by acting. We have so many cyber  
9 intrusions going on every day that there’s plenty of  
10 opportunity to act.

11 Senator Inhofe: Thank you.

12 Thank you, Mr. Chairman.

13 Chairman McCain: [Presiding] Senator Shaheen?

14 Senator Shaheen: Thank you, Mr. Chairman.

15 And thank you gentlemen for being here today.

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

22 I was in Poland with Senator Durbin last week, and one  
23 of the things that we heard from some of the civil society  
24 leaders in Poland was they were asking about the hacking of  
25 our electoral system, and they said if the United States

1 isn't going to take any action in response to that Russian  
2 intrusion against your elections, then how can we think that  
3 the United States is going to take any action to protect us  
4 against Russia?

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

12         Dr. Fields: I don't feel qualified to observe whether  
13 or not hacking into our election is an act of war or isn't  
14 an act of war.

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

18         Dr. Fields: I think the question that I'm worried  
19 about is what do we want to do so that it doesn't happen in  
20 2018 and doesn't happen in 2020. Taking no action  
21 guarantees escalation. Taking action has the possibility of  
22 escalation but also the possibility of deterrence. There  
23 are many possible actions we can take, not for this hearing,  
24 unclassified, but we have to do it.

25         Senator Shaheen: General Alexander?

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

12           Senator Shaheen:  Well, I certainly agree with that.  
13 That makes sense.

14           And to your point about cooperating with the private  
15 sector, the Department of Defense has issued regulations  
16 that require all DOD contractors, including small  
17 businesses, to comply with a series of cyber security  
18 requirements by December 31st of this year.  And as part of  
19 this rulemaking process, the Small Business Administration  
20 -- I sit on the Small Business Committee, so that's why this  
21 has come to my attention -- their Office of Advocacy has  
22 claimed that DOD underestimated the number of small  
23 businesses that are going to be affected by the rule, the  
24 costs of the rule, and the ability of small businesses to  
25 comply.  And in the final rule issued last October, DOD

1 claimed it was not feasible to implement recommendations  
2 from the Office of Advocacy to provide some financial help  
3 to small business and some guidance, and they admitted that  
4 the cost of complying with the rule was unknown.

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

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

14 General Alexander: So there are actually two sets of  
15 issues that you bring up. First, it is really difficult to  
16 comply with these types of standards. One is the  
17 international standard 27,001, one is the NIST framework.  
18 As you look at it, how do companies certify that they've met  
19 all of those? That's a year-long process. It's very  
20 expensive, and you need a lot of people to do it. So a  
21 small business that has five people, it's going to be  
22 difficult.

23 So I think we have to set up realistic expectations.  
24 How do they do that, or could they sub to a contractor who  
25 has that authority? And the answer is I think you can get

1 there. We are actually going through that in my company, so  
2 I can tell you how hard it is. We're doing it, and we have  
3 some people with perhaps some security background. So when  
4 we look at it, it's very difficult.

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

15 Senator Shaheen: Thank you.

16 Thank you, Mr. Chairman.

17 Chairman McCain: Thank you.

18 Senator Fischer?

19 Senator Fischer: Thank you, Mr. Chairman.

20 Dr. Miller and Dr. Fields, the Defense Science Board  
21 recently released a final report on cyber deterrence and  
22 included a recommendation that the commander of CYBERCOM  
23 should develop scalable and strategic offensive cyber  
24 capabilities in order to deter cyber attacks against our  
25 critical infrastructure here in this country. Can you

1 elaborate on this and what types of capabilities the DSB  
2 believes are needed, and tell us what the basis was for that  
3 recommendation?

4 Dr. Miller: Senator, the basis for the recommendation  
5 was that although the United States should have the  
6 available option of not just cyber but other responses,  
7 whether diplomatic, economic and so forth, that one of the  
8 most credible potential responses in offensive cyber in use  
9 against us is to use offensive cyber back against the state  
10 that undertook the attack. And following what Dr. Fields  
11 talked about, what we want to do in developing that  
12 portfolio of options to go against Russia or China or North  
13 Korea or Iran in particular is to look at the leadership  
14 values and to look across a range of potential targets that  
15 would hold at risk what they value. And then the value of  
16 having this, the campaign funding that we talked about, is  
17 to have a sense of what level of response and what specific  
18 types of targets might be most appropriate for a given  
19 scenario, and there's a risk of both doing too little,  
20 responding too weakly, and there's a risk of responding too  
21 strongly in the sense that in some instances you may want to  
22 reserve something to deter additional attacks.

23 So that's the fundamental structure of it, and as you  
24 look at those strategic options, the final point is to  
25 differentiate between those cyber actions by the military

1 that are intended to have tactical or operational level  
2 effects on the battlefield and those that are intended to  
3 have psychological effects on the leadership of our  
4 potential adversaries.

5 Senator Fischer: As you said in your opening, you're  
6 weighing the cost and the benefit, the increase and the  
7 decrease, on each of these; correct?

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

12 Senator Fischer: Another recommendation in the final  
13 report focused on acquisition of these offensive cyber  
14 capabilities. Specifically, it called for improved and  
15 accelerated acquisition authorities for CYBERCOM and also  
16 the establishment of a special organization for rapid  
17 acquisition.

18 In the Fiscal Year 2016 NDAA, the Emerging Threats and  
19 Capabilities Subcommittee, which I chaired at that time with  
20 Senator Nelson, included language that provided the  
21 commander of CYBERCOM some acquisition authority. In the  
22 Fiscal Year 2017 bill, it greatly expanded the commander's  
23 role in the requirement to process. I know some of the  
24 changes are still waiting to be implemented, but can you  
25 talk about how this dovetails with what the DSB was

1 thinking, and are there other areas where further  
2 congressional action would be helpful?

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

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

22 Senator Fischer: Thank you, sir.

23 Thank you, Mr. Chairman.

24 Chairman McCain: Thank you.

25 Senator Kaine?

1 Senator Kaine: Thank you, Mr. Chairman.

2 Thank you to the witnesses.

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

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

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

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

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

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

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

4           Senator Kaine: Other thoughts?

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

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

23           Senator Kaine: Yes, we want to counter it but counter  
24 it in accord with our values, not contrary to our values.

25           Dr. Fields: You were correct in noting that

1 information ops, influence ops of the sort you're talking  
2 about, go beyond cyber and not only include cyber. Some  
3 examples: a foreign power buying a television station so it  
4 can make its point of view known because television is so  
5 influential; making campaign contributions through cutouts  
6 to particular political candidates. It's widespread.

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

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

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

22 There is a similar program, a kind of ROTC type program  
23 that is done through the National Science Foundation called  
24 Cyber Corps. But are programs like this necessary to try to  
25 bring in the talent that we need to ultimately fill the

1 structure that we hope we might create that would be  
2 effective?

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

11 Dr. Fields: I would just add that there isn't a  
12 comprehensive program of the sort you're talking about and  
13 there should be. There are activities. DARPA was very,  
14 very active in trying to engage young people, holding  
15 contests, and it's really very effective, if not  
16 comprehensive.

17 Senator Kaine: Thank you.

18 Thank you, Mr. Chairman.

19 Chairman McCain: Thank you.

20 Senator Rounds?

21 Senator Rounds: Thank you, Mr. Chairman.

22 Mr. Waxman, I find it fascinating the discussion on  
23 sovereignty and the challenges that that would have for our  
24 country when we're talking about other players, whether they  
25 be first-tier competitors or non-country actors, non-

1 national actors. They don't seem to have much concern about  
2 whether or not they move through the cyber world in the  
3 sovereignty area of other countries, or at least those areas  
4 that may very well come through lines that are in other  
5 countries.

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

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

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

23 As you said, recently published is a book, an effort  
24 called TALLINN 2.0. This was something that was conducted  
25 under the auspices of NATO's Center of Excellence for cyber

1 issues, and it's an impressive and very important product  
2 for surveying the many international law issues that come  
3 up. I don't agree with all of its conclusions, though, and  
4 in particular I worry that it's an example of overly-  
5 restrictive interpretations of sovereignty that could  
6 needlessly and perhaps dangerously restrict our operational  
7 flexibility.

8 Senator Rounds: Thank you.

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

11 Dr. Miller: I don't want to give you a legal opinion  
12 because I'm not a lawyer, but I will say that some policy  
13 steps can be taken that can reduce that. For example, if we  
14 work with our allies and partners to have reciprocal  
15 arrangements where if we see something on their networks  
16 that's a threat we will take care of it, understanding that  
17 the presumption would be that there is no or minimal side  
18 effects associated with it, this could allow faster action,  
19 at least within that federation of allies and partners. I  
20 think there are a number of other steps that we should be  
21 looking at, and it reinforces Mr. Waxman's earlier point  
22 that the lawyers and policy people have to work closely  
23 together, and to do so in real time, the real world, and  
24 working through real problems.

25 Senator Rounds: Thank you.

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

12           General Alexander: Senator, I would take one step  
13 further and say, for example, ISIS and other terrorism on  
14 the network, we shouldn't allow it, and we should work with  
15 our allies. If they have anything on that network, we  
16 should all work to take it down and identify where it is and  
17 tell those countries to take it down.

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

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

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

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

21           Senator Rounds: Mr. Chairman, thank you.

22           Chairman McCain: Senator King?

23           Senator King: Thank you, Mr. Chairman. I think this  
24 may be the most important hearing that we've had since I've  
25 been here, and I want to put a fine point on that. To me,

1 the most chilling finding of the board was -- and this is a  
2 direct quote -- "The unfortunate reality is that for at  
3 least the next decade, the offensive cyber capabilities of  
4 our most capable adversaries are likely to far exceed the  
5 United States' ability to defend key critical  
6 infrastructure." That is a powerful statement, and it seems  
7 to me that what we are observing here is a fundamental  
8 change in the nature of warfare that's occurring right  
9 before our eyes.

10 The historical example I think of is the Battle of  
11 Agincourt in October of 1415, when a ragtag British army of  
12 7,000 soundly defeated a French army estimated between  
13 20,000 and 30,000. The British lost 600. The French lost  
14 7,000. And the difference was technology, the long bow.  
15 That is what changed the course of history, and it was  
16 because the mightiest army in the world, the French, did not  
17 wake up to the change in technology represented by the long  
18 bow.

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

1 jurisdiction together, I don't think anybody in Maine is  
2 going to buy that.

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

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

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

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

19 Senator King: Well, I think we've got to have the  
20 capacity to deter.

21 The other question, and this gets back to my comment  
22 about congressional jurisdiction and committees, does this  
23 need congressional action, or is this something the  
24 executive has responsibility for because of their being the  
25 Commander in Chief? Is this something that can be done

1 within the organization of the executive branch, or is there  
2 legislation necessary? And if there is, tell us what it is  
3 so we can move on it.

4 General Alexander?

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

10 Senator King: Much better, but do you think it's  
11 capable to defend entirely? I don't think that's possible  
12 technologically.

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

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

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

25 General Alexander: Right, so we ought to get on with

1 it. What we've done since seven years ago when I went  
2 before this committee -- thank you -- and you guys confirmed  
3 me despite all that, at that time we talked about defending  
4 this country. Here's how I think we should do it. Put  
5 together a framework, but also have the rules of engagement  
6 so when somebody comes at us, we go back at them.

7 Senator King: That gets to my point about it has to be  
8 public. People have to know what the rules are.

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

17 Senator King: I agree. Thank you.

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

22 I want to emphasize that it's fundamentally important  
23 to improve the defense and resilience of our critical  
24 infrastructure. It was the judgment of the task force that  
25 even with substantial efforts there, we are not going to be

1 able to prevent the most capable actors, by which I  
2 specifically mean China and Russia, from being able to --

3 Senator King: That was the sentence I read.

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

12 Chairman McCain: But doesn't this go back to what won  
13 the Cold War? Peace through strength. And if they commit  
14 one of these, a price, that they would pay for it, that it  
15 would be unacceptable. Rather than trying to devise --  
16 General Alexander said five years or so to construct the  
17 defenses. In the meantime, the response will be such that  
18 it will cost them a hell of a lot more than anything they  
19 might gain. Does that make any sense?

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

25 Chairman McCain: But as all the witnesses have said,

1 we don't want to create another bureaucracy, right?

2 Senator Wicker?

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

6 [Laughter.]

7 Senator King: "Oh, ye brothers, ye band of brothers,  
8 ye precious few."

9 Senator Wicker: But this is a different bunch we're  
10 talking about in this day and age.

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

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

23 Dr. Fields: To date, non-state actors haven't  
24 demonstrated the cyber power that the major state actors  
25 have demonstrated. That won't last forever, but it's the

1 case today.

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

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

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

22           As we think about terrorists groups, any groups that  
23 are willing to not just cause the loss of life but have its  
24 members lose their lives, whether through suicide bombings  
25 and so on, we really do need to focus on deterrence by

1 denial and a defensive posture. And as we think about that  
2 defensive posture, it's not just rope-a-dope. It's also the  
3 ability to preempt, as we do for other terrorist threats.

4 Senator Wicker: Deterrence by denial.

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

13 Senator Wicker: Yes, sir, General Alexander.

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

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

1           Senator Wicker: We haven't really sent very good  
2 signals the last few years about consequences and crossing  
3 lines.

4           Thank you, Mr. Chairman.

5           Chairman McCain: Senator Warren?

6           Senator Warren: Thank you, Mr. Chairman.

7           Thank you all for being here today.

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

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

22          So for 70 years the U.S. has had a policy of nuclear  
23 deterrence that has been a bedrock of our security. Given  
24 what happened last year, it seems clear that we need cyber  
25 deterrence, not just defense but deterrence as well. I know

1 that, Dr. Miller and Dr. Fields, you've issued a report on  
2 this. We want to talk about the organization of how that  
3 would work, but I want to ask a different question, and that  
4 is substantively, what should the United States do to deter  
5 these types of attacks in the future? At least describe  
6 somewhat the range of options that are available to us for  
7 deterrence, not defense but deterrence.

8 Dr. Miller?

9 Dr. Miller: Thank you, Senator. I'll defer coverage  
10 of some of the key elements. I'll just emphasize three of  
11 them in particular.

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

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

1           So first is a campaign planning construct.

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

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

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

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

1 Senator Warren: Dr. Fields, do you want to add  
2 something here?

3 Dr. Fields: I do, two things. Number one, we're not  
4 quite answering your question --

5 Senator Warren: Yes, that's right.

6 Dr. Fields: -- because we'd like to do so in closed  
7 session.

8 Senator Warren: All right. Fair enough.

9 Dr. Fields: We can in closed session.

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

17 Senator Warren: But doesn't that argue, then, even  
18 more strongly for a deterrence strategy?

19 Dr. Fields: Absolutely.

20 Senator Warren: Rather than relying exclusively on a  
21 defense strategy, and not confusing a defense strategy with  
22 a deterrent strategy, as I heard it discussed earlier?

23 Dr. Fields: That's why we did our study, and you'll  
24 notice that the study actually included some defense  
25 elements as well, but those would be for certain cases, for

1 certain actors, and really at a lower level. The top level  
2 should be deterrence.

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

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

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

20 Senator Warren: All right. That's very helpful.

21 I just want to say on this, nuclear deterrence works in  
22 part because we all knew it was out there. When we can't  
23 describe even in the most general terms what will happen if  
24 you engage in a cyber attack against us, and indeed it's  
25 clear that we have been the victims of a cyber attack by the

1 Russians, and we can't describe any kind of response to  
2 that, it seems to me that deterrence at that moment melts  
3 away to nothing. So I'm glad to take this into another  
4 setting to hear more about it, but there has to be some kind  
5 of response that is publicly known.

6 Thank you, Mr. Chairman.

7 Senator Peters: Thank you, Mr. Chairman.

8 Thank you to our panelists for a fascinating hearing  
9 here.

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

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

25 I know, Dr. Fields, you began to answer the question

1 and didn't have sufficient time. I'd like to give you some  
2 time now to tell us exactly what we should be doing.

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

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

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

19 Dr. Fields: That's also the case.

20 Senator Peters: So how do we deal with that?

21 Dr. Fields: There are going to be such cases. In  
22 fact, we can build systems, although we don't always do so,  
23 that are more fault tolerant, because many of the things  
24 that are put into microelectronics are very similar to what  
25 happens when a mistake is just an accidental mistake, and we

1 do work hard to design systems that compensate for  
2 accidental mistakes.

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

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

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

19 General Alexander: I think that's going to be a  
20 continuous work in progress, Senator. I think getting the  
21 information, because these systems are changing every couple  
22 of years, the technology that's going in, especially in the  
23 IT area, that's something that they have to be on top of.  
24 You bring out a good point. The cyber protection teams have  
25 to work with the customers they're supporting, and if we

1 look at where we put them, that may include industry as  
2 well, and parts of critical infrastructure.

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

6 Senator Peters: All right. Thank you.

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

19 I know that we have a range of tools to deal with this,  
20 including the CFIUS committee, but while the overall number  
21 of CFIUS reviews has risen steadily since 2008, the  
22 increase, as you know, is disproportionately small when  
23 compared to the ratio of completed transactions.

24 So, to the panel, if CFIUS is unable to slow China's  
25 advance, what are the implications for U.S. technological

1 superiority, in your mind?

2 Dr. Fields: My colleagues turned to me. We've done  
3 several studies on this over the years, we being the Defense  
4 Science Board, and I'm sorry to say that we've come up with  
5 no solution that I'll call a good solution. We have  
6 solutions for some things; not for this. In some areas we  
7 can continue to stay ahead. I'll call those areas software  
8 and some aspects of manufacturing. But this has proven to  
9 be a tough nut to crack. So I can offer you nothing that I  
10 have confidence in.

11 Senator Peters: A tough nut to crack, but one that we  
12 have to crack.

13 Dr. Fields: Yes.

14 Senator Peters: Thank you very much, appreciate it.

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

22 Mr. Waxman: Yes, Senator, I absolutely do. I think  
23 where I've seen it certainly very present is in legislative  
24 discussions about improving information sharing between the  
25 private sector and the government. I think pretty much

1 everybody agrees that that's critical to improving our cyber  
2 defenses, but I think the public and certainly segments of  
3 the public are very wary of sharing information with the  
4 government. Companies in some cases are leery of giving  
5 information to the government because they fear criticism on  
6 the civil liberties front.

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

11 Mr. Waxman: Yes, Senator.

12 Chairman McCain: And it's not easy.

13 Mr. Waxman: No, Senator.

14 Chairman McCain: But given the fact that you're a  
15 great lawyer, you're going to give us the answer. Is that  
16 right?

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

24 Chairman McCain: Well, General Alexander, on your  
25 watch, you gave us a lot of confidence, and we are very glad

1 that you are back here before the committee, and we will  
2 continue to call on you for your unique experience and  
3 knowledge.

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

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

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

23 Senator Reed?

24 Senator Reed: Mr. Chairman, I concur entirely. I  
25 thank you again for hosting this hearing. I think it's our

1 mutual desire and wish that these hearings lead to prompt  
2 remedial action, and I know with the Chairman's leadership  
3 that will happen. Thank you.

4 Chairman McCain: I thank the witnesses.

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

7 Thanks again.

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

9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25