

Stenographic Transcript  
Before the

COMMITTEE ON  
ARMED SERVICES

**UNITED STATES SENATE**

HEARING TO RECEIVE TESTIMONY ON  
ENCRYPTION AND CYBER MATTERS

Tuesday, September 13, 2016

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  
ENCRYPTION AND CYBER MATTERS

Tuesday, September 13, 2016

U.S. Senate  
Committee on Armed Services  
Washington, D.C.

The committee met, pursuant to notice, at 9:37 a.m. in Room SH-216, Hart Senate Office Building, Hon. John McCain, chairman of the committee, presiding.

Committee Members Present: Senators McCain [presiding], Wicker, Fischer, Cotton, Rounds, Ernst, Sullivan, Lee, Cruz, Reed, Nelson, McCaskill, Manchin, Shaheen, Gillibrand, Blumenthal, Donnelly, Hirono, King, and Heinrich.

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

3           Chairman McCain: I would -- since a quorum is not  
4 present, but we have pending military nominations, I would  
5 ask unanimous consent to waive the requirement for two  
6 more members in order to conduct a routine business for  
7 the 4,158 pending military nominations, which I'm -- none  
8 of which are controversial. Is there any objection to  
9 that?

10          [No response.]

11          Chairman McCain: If not, since -- a quorum is not  
12 present, but I ask the committee to consider a list of  
13 4,158 pending military nominations. Of these nominations,  
14 503 nominations are 2 days short of the committee's  
15 requirement that nominations be in committee for 7 days  
16 before we report them out. No objection has been raised.  
17 These nominations -- I recommend the committee waive the  
18 7-day rule in order to permit the confirmation of the  
19 nomination of these officers before the Senate goes out  
20 for the October recess.

21          Is there a motion to favorably report these 4,158  
22 military nominations to the Senate?

23          Senator Reed: So move.

24          Chairman McCain: Is there a second?

25          Senator Wicker: Second.

1 Chairman McCain: All in favor?

2 [A chorus of ayes.]

3 Chairman McCain: The motion carries.

4 And I thank the committee. We wouldn't want to go out  
5 for a long period of time with these pending nominations,  
6 none of which are in any way controversial.

7 And I think that there was a cyber attack on Admiral  
8 Rogers' automobile, which accounts for him being late this  
9 morning.

10 [Laughter.]

11 Chairman McCain: We'll have a full investigation --

12 Voice: He's joking.

13 [Laughter.]

14 Chairman McCain: Mr. Secretary, we welcome you and  
15 Admiral Rogers. And we'll begin with you, Mr. Secretary.

16 Mr. Lettre: Chairman McCain, Ranking Member Reed,  
17 members of the committee, thank you for inviting us to  
18 discuss the importance of strong encryption, trends on its  
19 use, and its impact on the Department of Defense.

20 With your permission, I've submitted a longer written  
21 statement, and I would ask that it be made part of today's  
22 record.

23 Chairman McCain: If you'll hold for a moment,  
24 Secretary Lettre, in my -- I forgot the opening statements  
25 by myself and the Ranking Member --

1 [Laughter.]

2 Mr. Lettre: I was wondering about that.

3 Chairman McCain: -- which is the reason why so many of  
4 my colleagues are staying here, in order to hear our words  
5 of wisdom.

6 [Laughter.]

7 Senator Nelson: We thought you were going to spare us.

8 [Laughter.]

9 Chairman McCain: Probably should, given the calendar,  
10 but could I just -- I'll go ahead, and we'll hold you,  
11 Senator -- Secretary Lettre.

12 Encryption has become ubiquitous across the  
13 counterterrorism fight. ISIL has successfully leveraged  
14 messaging applications developed by some of our most  
15 innovative companies to create an end-to-end encrypted  
16 safe haven where they can operate with near perfect  
17 secrecy and at arms' length of law enforcement, the  
18 intelligence community, and the military. From Syria to  
19 San Bernardino to Paris to Brussels to perhaps even  
20 Orlando, ISIL has utilized encrypted communications that,  
21 just a few years ago, were limited to a select few of the  
22 world's premier military and intelligence services.

23 As I've stated in the past, this is a complex and  
24 difficult problem, with no easy solutions. We must  
25 balance our national security needs and the rights of our

1 citizens. We must also recognize that authoritarian  
2 regimes are eager to gain keys to encrypted software so  
3 they can further their own abusive policies, such as  
4 suppressing dissent and violating basic human rights.  
5 Yet, ignoring the issue, as the White House has done, is  
6 also not an option.

7 I look forward to hearing how the use of encryption by  
8 terrorist organizations is impacting your ability to  
9 detect and prevent future attacks, and how the  
10 proliferation of encryption alters the way you do business  
11 at the NSA and Cyber Command.

12 Admiral Rogers, you have frequently spoken with this  
13 committee about the so-called "dual hat" under which the  
14 Commander of Cyber Command also serves as the Director of  
15 the NSA. Last year, you told this committee, quote, "I  
16 will strongly recommend, to anyone who asks, that we  
17 remain in the 'dual-hat' relationship. This is simply the  
18 right thing to do for now, as the White House reiterated  
19 in late 2013." You stated that it might not be a  
20 permanent solution, but that it is a good solution, given  
21 where we are. You were asked again in our hearing earlier  
22 this year, and you reaffirmed the need to keep the two  
23 organizations tightly aligned.

24 That's why I'm troubled by recent reports that the  
25 Obama administration may be trying to prematurely break

1 the dual-hat before Obama -- President Obama leaves  
2 office. On Friday, it was reported that Secretary of  
3 Defense Ash Carter and Director of National Intelligence  
4 James Clapper have backed a plan to separate Cyber Command  
5 and the NSA. Here we go again. Another major policy  
6 matter has apparently been decided, with no consultation  
7 whatsoever between the White House or the Department of  
8 Defense with this committee. I urged Secretary Carter to  
9 provide this committee and the Congress the details of  
10 this plan and his reasoning for support it. I will --  
11 hope he will explain what has changed since the last time  
12 the administration rejected this idea, in 2013.

13 And while I'm sure the phrase "predecisional" is  
14 written somewhere in our witnesses' briefing papers, I  
15 would remind them that this committee does not take well  
16 to being stonewalled while their colleagues in the  
17 administration leak information to the press. Even if  
18 this decision has not been made, our witnesses should  
19 still be able to provide substantive analysis on the  
20 consequences of separating the dual-hat for our national  
21 security and for taxpayers.

22 Let me be very clear. I do not believe rushing to  
23 separate the dual-hat in the final months of an  
24 administration is appropriate, given the very serious  
25 challenges we face in cyberspace and the failure of this

1 administration to develop an effective deterrence policy.  
2 Therefore, if a decision is prematurely made to separate  
3 NSA and Cyber Command, I will object to the confirmation  
4 of any individual nominated by the President to replace  
5 the Director of the National Security Agency if that  
6 person is not also nominated to be the Commander of Cyber  
7 Command.

8 This committee and this Chairman are tired of the way  
9 that Congress, in general, and this committee is treated  
10 by this administration. These issues present larger  
11 concerns about whether the Department is appropriately  
12 organized to manage the defensive and offensive  
13 requirements of the cyber mission. We know that the  
14 Department faces challenges in recruiting and retaining  
15 top cyber talent. We know that the Department's  
16 cumbersome acquisition system hinders technological  
17 advancement and has eroded our technological superiority.  
18 And we know that the administration's failure to confront  
19 deficiencies in its cyber policy has undermined the  
20 Department's ability to effectively defend, deter, and  
21 respond to our adversaries in cyberspace. Both Russia and  
22 China have leveraged cyber to systematically pillage  
23 certain critical defense technologies, create uncertainty  
24 in our networks, and demonstrate capability. Make no  
25 mistake, they are the first movers in the cyber domain,

1 and they have put us on the defensive. But, the  
2 administration has consistently failed to provide a  
3 meaningful response.

4 The latest media reporting, that Russia may try to  
5 undermine our electoral process, underscores this point.  
6 Russia is using cyber to undermine American national  
7 interest, and now it appears our democracy could be the  
8 next target. And the administration's response to a mere  
9 warning from the Secretary of Defense -- is that the best  
10 the United States can do? Despite this committee's  
11 numerous requests for a cyber deterrence framework, the  
12 administration has failed to present any meaningful  
13 strategy. Instead, it has evidently distracted itself  
14 with debates over the dual-hat. Instead of shaping the  
15 limits of acceptable behavior in cyberspace, the  
16 administration, instead, has allowed Russia and China to  
17 write the playbook. As a result, this administration has  
18 left the United States vulnerable.

19 I look forward to hearing more about the cyber  
20 operations against ISIL and the challenges, opportunities,  
21 and constraints you are facing on the cyber front.

22 Senator Reed.

23

24

25

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

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

4           Let me join you in welcoming Secretary Lettre and  
5 Admiral Rogers to -- back to the committee.

6           Thank you, gentlemen, and the men and women that you  
7 lead, for their service and your service.

8           This is a third committee hearing focused on the  
9 encryption issue, which underscores the importance of this  
10 issue and its impact on national security. The rapid  
11 growth of sophisticated end-to-end encryption applications  
12 and extremely secure physical access control to  
13 smartphones and computers has an adverse impact on law  
14 enforcement agencies at all level of government, and  
15 impairs the ability of the intelligence community and the  
16 Defense Department's Cyber Command to detect and counter  
17 cyber threats to the Nation. At the same time, this  
18 security technology helps to protect individuals,  
19 corporations, and the government against cybercrime,  
20 espionage, terrorism, and aggression.

21           While FBI Director Comey has tirelessly stressed the  
22 danger of law enforcement going dark, respected national  
23 security experts, including General Michael Hayden, former  
24 Director CIA and NSA, Michael Chertoff, the former Under  
25 Secretary -- or Secretary, rather, of Homeland Security,

1 have advised against compelling industry to ensure that  
2 the government can always get access to encrypted data.  
3 These experts argue that cyber vulnerabilities are the  
4 greatest threat to the public and national security. And  
5 this debate underscores the complexity and difficulty of  
6 the issue that we all face and we all must deal with very  
7 quickly, because it is a growing -- as the Chairman's  
8 testimony indicates, it's a growing threat to our national  
9 security and our law enforcement.

10 A major problem for law enforcement at this juncture is  
11 gaining access to data on devices that are physically in  
12 their control for foreign intelligence collection, where  
13 physical access is rarely, if ever, applicable, the  
14 challenges to overcome encryption of data in transit, or  
15 to gain remote access to devices when they are turned on  
16 and communicating. And the latter set of problems is not  
17 qualitatively new. And I will ask, when questioning,  
18 whether they're more manageable than these law enforcement  
19 issues.

20 In addition to encryption, another important area that  
21 I hope we're able to discuss today is the issue that the  
22 Chairman brought up. That's the future of Cyber Command.  
23 I understand the administration is deliberating on whether  
24 it is the proper time to elevate Cyber Command to a  
25 unified command, and if, and under what conditions, the

1 administration should terminate the so-called "dual-hat"  
2 arrangement in which the Commander of Cyber Command serves  
3 also as the Director of the NSA. An additional issue, a  
4 discussion of whether the Director of NSA should be a  
5 civilian rather than a general officer. And, while I know  
6 that is likely difficult for our witnesses to discuss  
7 administrative deliberations in an open hearing, I will  
8 welcome any of your thoughts or considerations on these  
9 important issues.

10 Another area that I know is of interest to the  
11 committee, but, again, may be difficult to comment on  
12 publicly, is several revelations of hacking of major  
13 computer systems in this country by outside actors.  
14 Again, that is a very critical issue and one that we're  
15 very much involved and interested in.

16 Once again, gentlemen, thank you for your service, and  
17 thank you for your appearance here today.

18 Chairman McCain: Now Secretary Lettre.

19  
20  
21  
22  
23  
24  
25

1           STATEMENT OF HON. MARCELL J. LETTRE II, UNDER  
2           SECRETARY OF DEFENSE FOR INTELLIGENCE

3           Mr. Lettre: Chairman McCain, Ranking Member Reed, and  
4           members of the committee, thank you for inviting us to  
5           discuss the importance of strong encryption, trends on its  
6           use, and its impact on the Department of Defense.

7           With your permission, I have a written statement that  
8           is a little longer than my opening statement here, and I'd  
9           ask that it be made part of today's record.

10          In my brief opening statement, I would like to  
11          underscore three points:

12          First, the Department of Defense strongly seeks robust  
13          encryption standards and technology vital to protecting  
14          our warfighting capabilities and ensuring that key data  
15          systems remain secure and impenetrable to our adversaries  
16          today and well into the future. The Department's support  
17          for the use of strong encryption goes well beyond its  
18          obvious military value. For example, commercial  
19          encryption technology is not only essential to U.S.  
20          economic security and competitiveness, but the Department  
21          depends upon our commercial partners and contractors to  
22          help protect national security systems, research-and-  
23          development data related to our weapon systems, classified  
24          and sensitive information, and service members' and  
25          Department civilians' personally identifiable information

1 and health records.

2 Second, we are concerned about adversaries,  
3 particularly terrorist actors, using technology  
4 innovation, including ubiquitous encryption, to do harm to  
5 Americans. The cybersecurity challenges confronting the  
6 Department are compounded by the pace and scope of change,  
7 not only in the threat environment, but also in associated  
8 technologies. Our adversaries are constantly searching,  
9 looking, and adopting new and widely available encryption  
10 capabilities, with terrorist groups such as the Islamic  
11 State of Iraq in the Levant, ISIL, leveraging such  
12 technology to recruit, plan, and conduct operations. Our  
13 concern grows as some parts of the communication  
14 technology industry move towards encryption systems that  
15 providers themselves are incapable of un-encrypting, even  
16 when served with lawful government requests to do so for  
17 law enforcement or national security needs. This presents  
18 a unique policy challenge, one that requires that we  
19 carefully review how we manage the tradeoffs inherent in  
20 protecting our values, which include individual privacy as  
21 well as our support for U.S. companies' ability to  
22 innovate and compete the global economy, and also  
23 protecting our citizens from those who mean to do us grave  
24 harm.

25 Third, the Department is working with other parts of

1 the government and the private sector to seek appropriate  
2 solutions on these issues now. We need to strengthen our  
3 partnership with the private sector, finding ways to  
4 protect our systems against our adversaries' cyberattacks  
5 and at the same time finding innovative and broadly  
6 acceptable ways to address nefarious actors' adoption of  
7 new technologies, including encryption, even while we must  
8 carefully avoid introducing any unintentional weaknesses  
9 in the protection of our security systems or hurting our  
10 global economic competitiveness.

11 Mr. Chairman, the Department is committed to the  
12 security and resiliency of our data and networks, and to  
13 defending the U.S. at home and abroad. An ongoing  
14 dialogue with Congress as well as other departments and  
15 agencies and the private sector is absolutely critical as  
16 we work together to confront and overcome the security  
17 challenges associated with encryption.

18 I appreciate the committee's interest in these issues,  
19 grateful for the dialogue, and I look forward to your  
20 questions.

21 [The prepared statement of Mr. Lettre follows:]

22

23

24

25

1 Chairman McCain: Admiral Rogers.  
2  
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 ADMIRAL MICHAEL S. ROGERS, USN,  
2           COMMANDER, UNITED STATES CYBER COMMAND; DIRECTOR, NATIONAL  
3           SECURITY AGENCY; CHIEF, CENTRAL SECURITY SERVICES

4           Admiral Rogers: Chairman McCain, Ranking Member Reed,  
5           and members of the committee, thank you for the  
6           opportunity to appear before you today to discuss the  
7           current communications environment, including strong  
8           encryption and cyber challenges.

9           When we last met, on the 12th of July in a closed  
10          session, I outlined several of those challenges to the  
11          committee. And today, I look forward to further  
12          discussion so the American people are provided the  
13          greatest amount of information possible on these important  
14          topics. Of course, some aspects of what we do must remain  
15          classified to protect national security, so today I will  
16          limit my discussion to those in the public domain.

17          When I use the term "encryption," I'm referring to a  
18          means to protect data from any access except by those who  
19          are authorized to have it. Encryption is usually done by  
20          combining random data with the data you want to protect.  
21          The random data is generated by a mathematical algorithm  
22          and uses some secret information only, called a key, in  
23          the generation. Without the key, you can't undo the  
24          encryption.

25          NSA supports the use of encryption. It's fundamental

1 to the protection of everyone's data as it travels across  
2 the global network. NSA, through its information  
3 assurance mission, for example, sets the encryption  
4 standards within the Department of Defense. We understand  
5 encryption. We rely on it, ourselves, and set the  
6 standards for others in the U.S. Government to use it  
7 properly to protect national security systems. At the  
8 same time, we acknowledge encryption presents an ever-  
9 increasing challenge to the foreign intelligence mission  
10 of NSA. The easy availability of strong encryption by  
11 those who wish to harm our citizens, our government, and  
12 our allies is a threat to our national security. As you  
13 well know, the threat environment, both in cyberspace and  
14 in the physical world, is constantly evolving, and we must  
15 keep pace in order to provide policymakers and warfighters  
16 the foreign intelligence they need to help keep us safe.

17 Terrorists and other adversary tactics, techniques, and  
18 procedures continue to evolve. Those who would seek to  
19 harm us, whether they be terrorists or criminals, use the  
20 same Internet, the same mobile communication devices, the  
21 same software and applications, and the same social media  
22 platforms that law-abiding citizens around the world use.  
23 The trend is clear. The adversaries continue to get  
24 better at protecting their communications, including  
25 through the use of strong encryption.

1 I want to take this opportunity to assure you and the  
2 American people that the NSA has not stood still in  
3 response to this changing threat environment. We are  
4 making investments in technologies and capabilities  
5 designed to help us address this challenge. And last  
6 year, we started a process to better help position  
7 ourselves to face these challenges.

8 It is premised in the idea that, as good as NSA is --  
9 as it is at foreign intelligence and its information  
10 assurance mission, the world will continue to change. And  
11 the goal is, therefore, to change, as well, to ensure that  
12 we will be as effective tomorrow as we are today. The  
13 Nation counts on NSA to achieve insights into what is  
14 happening in the world around us, what should be of  
15 concern to our Nation's security, the safety and well-  
16 being of our citizens and of our friends and allies.

17 We have a challenge before us. We are watching  
18 sophisticated adversaries change their communication  
19 profiles in ways that enable them to hide information  
20 relating to their involvement in things such as criminal  
21 behavior, terrorist planning, malicious cyber intrusions,  
22 and even cyberattacks. Right now, technology enables them  
23 to communicate in a way that is increasingly problematic  
24 for NSA and others to acquire critical foreign  
25 intelligence needed to protect the Nation or for law

1 enforcement individuals to defend our Nation from criminal  
2 activity.

3 The question then becomes, So what's the best way to  
4 deal with this? Encryption is foundational to the future.  
5 The challenge becomes, given that premise, What is the  
6 best way for us ensure the protection of information, the  
7 privacy and civil liberties of our citizens, and the  
8 production of the foreign intelligence necessary to ensure  
9 those citizens' protection and safety? All three are  
10 incredibly important to us as a Nation.

11 You've also asked me to talk about cyber deterrence and  
12 U.S. Cyber Command's organizational structure. As I have  
13 said before, I do not believe that malicious cyber  
14 activity by adversaries can only be, or must be, deterred  
15 by cyber activity. Our Nation can deter by imposing costs  
16 in and through other domains as well as using a whole-of-  
17 nation approach. Our instruments -- all instruments of  
18 power should be considered when countering cyber threats,  
19 intrusions, or attacks.

20 And with regard to our organizational structure, U.S.  
21 Cyber Command is well along in building our Cyber Mission  
22 Force, deploying teams to defend the vital networks that  
23 undergird DOD operations to support combatant commanders  
24 in their missions worldwide, and to bolster DOD's capacity  
25 and capabilities to defend the Nation against cyberattacks

1 of significant consequence.

2 I, too, ask that my previously submitted written  
3 statement be made a part of the record.

4 And I look forward to your questions, sir.

5 [The prepared statement of Admiral Rogers follows:]

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 Chairman McCain: Thank you very much, Admiral. Is it  
2 still your professional military advice that maintaining  
3 the dual-hat at the -- at this time is in our best  
4 national security interest?

5 Admiral Rogers: Yes.

6 Chairman McCain: General Dempsey stated that cyber is  
7 the one area we lack an advantage over our adversaries.  
8 Do you agree -- still agree with that statement, Mr.  
9 Secretary?

10 Mr. Lettre: I do agree that cyber -- that the cyber  
11 threat is one of the greatest challenges we face.

12 Chairman McCain: Admiral?

13 Admiral Rogers: Yes.

14 Chairman McCain: Russian activity reporting hacking on  
15 our electoral process, I find it interesting that one of  
16 the two States there seems to be evidence of it is the  
17 State of Arizona. What can you tell us about the Russian  
18 activity and reported hacking on our electoral process?  
19 And do you think this is acceptable?

20 Admiral Rogers?

21 Admiral Rogers: Sir, as this is an ongoing  
22 investigation and a public, unclassified forum, I'm not  
23 going to be able to provide you specifics as to what our  
24 current assessment is. I will say this. This continues  
25 to be an issue of great focus, both for the foreign

1 intelligence community, attempting to generate insights as  
2 to what foreign nations are doing in this area, as --

3 Chairman McCain: This is the first time we've seen  
4 attempted interference in an -- in elections in the United  
5 States of America, isn't it, Admiral?

6 Admiral Rogers: Sir, we continue to see activity of  
7 concern. Again, I'm not going to characterize this  
8 activity "Is it a foreign nation-state, or not?"

9 Chairman McCain: Mr. Secretary, you have anything to  
10 add to that?

11 Mr. Lettre: Senator, I just would underscore that  
12 these are activities that the government is taking quite  
13 seriously. The FBI and the Department of Homeland  
14 Security has an aggressive investigation underway, so the  
15 government can form its conclusion.

16 Chairman McCain: Do we have a policy as to how to  
17 respond to this interference in elections in the United  
18 States of America? Do we have a policy as to what our  
19 actions be taken?

20 Mr. Secretary?

21 Mr. Lettre: In this particular instance, Senator, the  
22 government is intending to rely on the results of the  
23 investigation being led by the Bureau to --

24 Chairman McCain: I'm asking if --

25 Mr. Lettre: -- inform its policy decisions.

1 Chairman McCain: -- we have a policy, and the answer  
2 is no.

3 Admiral Rogers, there's a Wall Street Journal article  
4 yesterday, "New Tricks Make ISIS, Once Easily Tracked, a  
5 Sophisticated Opponent." Goes on and talks about how  
6 incredibly sophisticated some of their work was in  
7 preparation for these attacks -- electronic silences; when  
8 they did communicate, called or sent text messages;  
9 location; cheap burner phones, et cetera. What are we --  
10 what would you think about this kind of activity, Admiral?

11 Admiral Rogers: ISIL remains the most adaptive target  
12 I've ever worked in 35 years as an intelligence  
13 professional, sir.

14 Chairman McCain: So, it was -- is not a leap of the  
15 imagination to think that this kind of activity and  
16 planning further attacks on the United States is taking  
17 place as we speak?

18 Admiral Rogers: Yes, sir.

19 Chairman McCain: Admiral Rogers and Mr. Secretary, do  
20 you believe there's a legislative solution that can  
21 address some of these challenges we're talking about?

22 Mr. Lettre: Senator, it -- from my view, the  
23 legislative route is not something that we think is the  
24 best way to go, at this time. New legal and regulatory  
25 approaches are not as potentially productive as a robust

1 dialogue seeking cooperation and collaboration with the  
2 private sector.

3 Chairman McCain: I agree. And unless there is a  
4 policy about what the United States actions will be in the  
5 case of a threat, in the case of actual attack, in the  
6 case of other aspects of this challenge we're on, then  
7 you're going to see legislation. Right now, there is no  
8 policy. There is no policy that you can describe to me as  
9 to what we would do about an impending attack or what we  
10 would do about an attack. And so, there's a vacuum there.  
11 So, if you don't act, then I guarantee you the Congress  
12 will act.

13 Admiral Rogers, it was recently reported that Twitter  
14 barred Data Miner, a company specializing in searching  
15 across millions of Tweets to identify unfolding terrorist  
16 attacks and political unrest, from accessing its realtime  
17 stream of Tweets because of its work for U.S. intelligence  
18 agencies. According to an article in the Wall Street  
19 Journal, this service gave the U.S. Intelligence Committee  
20 -- community an alert about the Paris terrorist attacks  
21 shortly before they began to unfold last November. In  
22 March, the company says -- first notified clients about  
23 the Brussels attacks 10 minutes ahead. It also appears  
24 that Twitter will continue allowing information to be sold  
25 for use in the private sector, not just the government.

1 Help me out, here.

2 Admiral Rogers: I wish I could, Senator. I am  
3 perplexed by their approach in this particular instance.

4 Chairman McCain: So, we have a situation where --  
5 excuse me -- we have a situation where we have the ability  
6 to detect terror attacks using organizations such as Data  
7 Miner, and yet, in order for us to anticipate these  
8 attacks, we have to have certain information. And Twitter  
9 is refusing to allow them to have information which  
10 literally could prevent attacks on the United States of  
11 America? Is that the situation here, Admiral?

12 Admiral Rogers: Yes, sir. And at the same time, still  
13 willing to provide that information to others for business  
14 purposes.

15 Chairman McCain: For sale.

16 Admiral Rogers: For sale, for revenue.

17 Chairman McCain: What do you think we ought to do  
18 about people like that, besides expose -- besides exposing  
19 them for what they are?

20 Admiral Rogers: Clearly, I wish I had better  
21 understanding -- and perhaps there's insights that I'm  
22 just not aware of -- I wish I had better understanding as  
23 to the rationale that leads someone to believe that that  
24 is the right course of action. I'm just the first to  
25 acknowledge, I don't understand it.

1 Chairman McCain: So, shame on them.

2 Senator Reed.

3 Senator Reed: Thank you very much, Mr. Chairman.

4 And one of the issues -- and it's the last line of  
5 questioning, and it's highlighted quite a bit -- is that  
6 what used to be the domain of nation-states --  
7 sophisticated research, development, application of  
8 products -- are now done commercially all across the  
9 globe. I mean, some of these encryption devices were just  
10 adapted by ISIL, they weren't developed by ISIL, but  
11 they've been very effective. So, we're in a race not just  
12 against another nation-state, we're in a race against  
13 technical innovation that is widespread and is relatively  
14 inexpensive, in terms of the commitment you have to make  
15 to develop a product. Is that a fair assessment, Admiral  
16 Rogers?

17 Admiral Rogers: Yes, sir. I often use the phrase,  
18 "Cyber is the great equalizer." It doesn't take billions  
19 of dollars of investment, it doesn't take tens of  
20 thousands of dedicated individuals, and it's -- uses a set  
21 of capabilities that are readily available globally to a  
22 host of actors.

23 Senator Reed: And so, I think it's incumbent upon us  
24 to approach it not as we've done in the past, you know, a  
25 nation-state, to countering their technology, but with a

1 much more, you know, innovative approach.

2 So -- and let me ask both you and the Secretary, What  
3 is this new innovative approach to counter this new  
4 decentralized, disaggregated, relatively inexpensive  
5 ability to upset our very expensive and elaborate systems,  
6 both platforms and intelligence systems?

7 Mr. Lettre: Senator, I'd just make a couple of broad  
8 points on this.

9 The most important thing we need to do in the  
10 Department of Defense is reach out to any and all partners  
11 that can help us find solutions. For example, the  
12 Department's senior leadership has invested heavily in  
13 conversations with leadership across the U.S. technology  
14 sector to really seek a dialogue about how we can come up  
15 with innovative solutions to address the dynamics you've  
16 raised, which include a quick and agile set of adversaries  
17 being able to adapt to new technologies, themselves, and  
18 leveraging those technologies to conduct global messaging  
19 that advances their interests. We've got to find a way to  
20 outpace that. And we believe that we can do so by tapping  
21 into the best ingenuity that the American private sector  
22 has to offer.

23 Senator Reed: Admiral?

24 Admiral Rogers: The other thing we're trying to do, at  
25 an operational level, in addition to the power of

1 partnerships, which I agree with Marcell is very important  
2 for us -- the argument I'm trying to make on both the NSA  
3 and the Cyber Command side is, "Guys, we're dealing with a  
4 whole new ecosystem out there, and we've got to bore into  
5 this ecosystem and look at it in just that way. Don't  
6 focus on just one particular application as used by one  
7 particular target. Think more broadly about the host of  
8 actors that are out there, about how that" -- and I  
9 apologize, I can't get onto specifics in an open forum,  
10 but looking at it more deeply, not just the one particular  
11 app, if you will, used by one particular target, that if  
12 we look at this more as an ecosystem, we will find  
13 vulnerabilities that we can access to generate the  
14 insights that the Nation and our allies is counting on.

15 Senator Reed: But, I think, fundamental to your  
16 approach -- and again, it touches on the issues raised by  
17 the Chairman -- is that if these large technological  
18 players or, you know, civilian potential partners refuse  
19 to cooperate, then that is very -- could be detrimental in  
20 our security. And we have to find a way either to  
21 convince them or otherwise get them to cooperate, because  
22 I -- my sense is, without it, that we will not be able to  
23 deal with this issue. Is that fair?

24 Admiral Rogers?

25 Admiral Rogers: It is, from my perspective.

1 Partnerships is going to be incredibly foundational to the  
2 future, here.

3 Senator Reed: Just a final point. Raise it. You  
4 might comment quickly. That is, you know, there's been  
5 some discussion about having sort of a key to these  
6 encryption so that -- you know, the proverbial backdoor --  
7 so that government could get in, et cetera. Opponents to  
8 that approach suggest that that -- not only government  
9 could get in, but other bad actors could get in. So, is  
10 that a solution that causes more problems, or is that a  
11 real solution?

12 Mr. Lettre: Senator, from a policy perspective, we're  
13 in favor of strong encryption. We benefit from it,  
14 ourselves. So, anything that looks like a backdoor is not  
15 something we would like to pursue. The important thing, I  
16 think, is, on a case-by-case basis, for institutions like  
17 the Department of Defense and the Federal Bureau of  
18 Investigation and other key stakeholders, to have a really  
19 rich dialogue, case by case, with key industry players to  
20 see what kinds of solutions can be brought to bear, given  
21 the imperative to also balance privacy and civil liberties  
22 for our public, as well as to be able to ensure the  
23 competitiveness of our economic players.

24 Senator Reed: Thank you.

25 Thank you, Mr. Chairman.

1 Chairman McCain: If I -- Senator Rounds will indulge  
2 me one second.

3 Admiral, I just want to go back to this election in  
4 Arizona. Is it possible that Russians could somehow harm  
5 the electoral process in my home State of Arizona?

6 Admiral Rogers: Senator, let me plead ignorance on the  
7 specifics of the electoral system in the State of Arizona.

8 Chairman McCain: Or is it -- is there a possible  
9 scenario where they could disrupt the voting results in  
10 the upcoming election?

11 Admiral Rogers: I think there are scenarios where you  
12 can see capability applied in particular areas. Again,  
13 it's not -- I don't have strong fundamental knowledge  
14 across the breadth of the 50 States, since elections are  
15 run on a --

16 Chairman McCain: Yeah.

17 Admiral Rogers: -- State basis. And one advantage I  
18 do see, from a defensive standpoint, is that the structure  
19 is so disparate, with some elements being very -- still  
20 very manually focused, others being more electronically  
21 and interconnected -- because it's not just one  
22 nationwide, single, integrated structure, that tends to  
23 help us, I think, defensively, here.

24 Chairman McCain: But, it is a concern.

25 Admiral Rogers: Oh, yes, sir.

1 Chairman McCain: Senator Rounds. Thank you, Senator  
2 Rounds.

3 Senator Rounds: Thank you, Mr. Chairman. And thank  
4 you, to you and the Ranking Member, for putting this  
5 subject before us today.

6 I have a number of questions concerning how we respond  
7 to a cyberattack on civilian infrastructure. And I'm just  
8 curious. I know that the Chairman has already raised the  
9 question of a policy, but I'd like to go a little bit  
10 deeper. And what I'm really curious about is, what is the  
11 role of the Department of Defense with regard to an attack  
12 on civilian critical infrastructure? Is there a  
13 preemptive responsibility that the Department of Defense  
14 has to protect civilian infrastructure in a cyberattack,  
15 similar to what happens with a kinetic attack?

16 Mr. Lettre: Senator, from a policy perspective at DOD,  
17 we have three main missions. One is to defend the Defense  
18 Department and its networks. The second is to support our  
19 commanders in providing military options in support of  
20 their plans and operations that relate to cyber. And the  
21 third is, when called upon by the President and the  
22 national command leadership, to support broader efforts  
23 that might be brought to bear in the case of an attack on  
24 U.S. critical infrastructure.

25 Senator Rounds: Has that occurred? Has that request

1 occurred yet?

2 Mr. Lettre: Well, it -- the request typically would  
3 come in, in a specific instance of an attack.

4 Senator Rounds: So, in the case of an attack on a  
5 civilian infrastructure, how long would it take from the  
6 time that the attack is initiated until a time that the  
7 damage is done? Milliseconds?

8 Mr. Lettre: It really depends on the circumstances of  
9 the attack, but it can be pretty quick, in the case of a  
10 cyberattack, yes.

11 Senator Rounds: So, how in the world would we expect  
12 the President of the United States, even if it's not at  
13 3:00 o'clock in the morning, to respond in time to give  
14 you permission to protect critical civilian infrastructure  
15 if you already don't have a plan in place? Or do you have  
16 a plan in place?

17 Mr. Lettre: Right. And there -- at the policy level,  
18 there has been a multiyear effort to develop that overall  
19 framework for how to respond to attacks.

20 Senator Rounds: No --

21 Mr. Lettre: And then operationally --

22 Senator Rounds: -- either you've got one --

23 Mr. Lettre: -- there are systems, as well.

24 Senator Rounds: -- in place today or you do not. Do  
25 you have a plan in place today to respond to an attack on

1 critical civilian infrastructure?

2 Mr. Lettre: I believe we do have a plan in place,  
3 Senator. In July, for example, the President approved  
4 something called the Presidential Policy Directive on  
5 Cyberincident Coordination, PPD-41, which lays out a  
6 framework for an interagency effort to respond to attacks  
7 on our critical infrastructure from a cyber perspective.

8 Senator Rounds: So, you would not have to respond --

9 Mr. Lettre: In addition --

10 Senator Rounds: -- you would not have to wait for a  
11 presidential directive to protect critical infrastructure  
12 today.

13 Mr. Lettre: That's right. Now, there are a whole host  
14 of operational implications that need to follow from that.  
15 Each department and agency has worked through what  
16 capabilities it brings to bear and how quickly,  
17 operationally, those can be applied. In the case of the  
18 Department of Defense, obviously, we look very quickly to  
19 the capabilities of U.S. Cyber Command.

20 Senator Rounds: Admiral Rogers, today --

21 Admiral Rogers: Sir.

22 Senator Rounds: -- can we protect critical  
23 infrastructure if it is under a cyberattack?

24 Admiral Rogers: Do I have the capability to protect  
25 aspects of critical U.S. infrastructure? Yes, sir.

1 Senator Rounds: Thank you.

2 Let me go back. I -- you know, in the news, you've all  
3 heard, and we've all heard, about the discussions  
4 regarding Secretary Clinton's use of the email systems and  
5 so forth. One of the things that concerns me -- and I'd  
6 just like you to maybe put this in perspective for me if  
7 you could -- one of the ways in which we lose information  
8 or in which data that is private, confidential, classified  
9 is released, is not necessarily through unfriendly actors  
10 getting a hold of or breaking into our encrypted  
11 information, but simply human error and individuals within  
12 government who have access to classified or confidential  
13 information, or information which is classified at a  
14 higher category than that. Could you talk to us a little  
15 bit about what the responsibility is and whose  
16 responsibility it is to actually train or to give  
17 information to individuals who are either elected,  
18 appointed, or hired by the government to make sure that  
19 they understand the differences between the categories,  
20 between whether a "C" means that it's in alphabetical  
21 order or it is Confidential or any classified setting?  
22 Whose responsibility is it within the governmental layout,  
23 the structure today, to see that that information is  
24 appropriately disseminated and that instructions and  
25 remedial instructions are provided if there is a break?

1 Where does that fit?

2 Mr. Lettre: Senator, the questions around cyber  
3 hygiene, essentially, and how to properly protect yourself  
4 against IT intrusions and so forth is one set of policies  
5 and practices that typically the CIOs and associated IT  
6 security managers have responsibility for educating  
7 government employees at all levels. There are also  
8 aspects around the handling of classified information that  
9 flow from security policies and procedures, and those are  
10 typically handled by departments' security subject-matter  
11 experts.

12 Senator Rounds: Department by department?

13 Mr. Lettre: Typically so, yes, sir.

14 Senator Rounds: And who oversees that information --  
15 or the delivery of that information?

16 Mr. Lettre: Well, the --

17 Senator Rounds: Your agency?

18 Mr. Lettre: The -- in the case of the Department of  
19 Defense, for DOD employees, my office oversees the setting  
20 of security policy standards.

21 Senator Rounds: Mr. Chairman, thank you.

22 Chairman McCain: Senator Nelson.

23 Senator Nelson: Admiral, I have often thought of our  
24 ability to protect ourselves in cyber as that we are  
25 really almost like the standoff in the nuclear, assured

1 mutual destruction. It gets more complicated with this,  
2 because we have nonstate actors. But, could you give us  
3 an example, in this open setting -- and, if required, then  
4 in a classified setting -- of where we have been attacked  
5 and we showed them that the return hit is going to be so  
6 hard that it deters them from hitting in the future?

7 Admiral Rogers: Again, I can't get any details in an  
8 open forum, but I would suggest the response to the Sony  
9 hack by the North Koreans in November of 2014 is an  
10 example of that.

11 Senator Nelson: And is that in the public domain --  
12 that example?

13 Admiral Rogers: In the sense that we publicly  
14 acknowledged both the event, we publicly acknowledged who  
15 did it, and we publicly discussed the steps we were going  
16 to take in response to it, and we also highlighted at the  
17 time, "And if this activity continues, we are prepared to  
18 do more at the time and place of our choosing."

19 Senator Nelson: And the specifics of that, will that  
20 have to be in a classified setting?

21 Admiral Rogers: No, in the sense that, in this case,  
22 we chose to use the economic lever, it goes to one of the  
23 comments I made in my opening statement. One of the  
24 things I'm always recommending -- I realize I just work  
25 the operational piece of much of this -- but, I always

1 encourage people, "Think more broadly than cyber. When  
2 thinking deterrence, think more broadly than cyber." Just  
3 because an entity, nation-state, group, individual comes  
4 at us in cyber, that doesn't mean that our response has to  
5 automatically fall back on, "Well, we have to respond in  
6 kind. We have to go back from a cyber perspective." I've  
7 tried to make the argument, as have others, we need to  
8 play to all of the strengths of our Nation. So, in the  
9 Sony case, for example, we collectively, from a policy  
10 perspective, made a choice to play to the strength of the  
11 economic piece for the United States.

12 Senator Nelson: Right. And I think that's smart.  
13 You've got a menu of things.

14 Admiral Rogers: Sir.

15 Senator Nelson: But, when you get right down to tit-  
16 for-tat, we could absolutely, with our attacks, shut down  
17 a number of things.

18 Admiral Rogers: We could cause significant challenges  
19 to an opponent. I'm not going to get into specifics, but  
20 yes.

21 Senator Nelson: Right. So, do -- with state actors,  
22 do we see that that is actually creating a mutually  
23 assured destruction?

24 Admiral Rogers: I would argue, not yet. Because  
25 remember, a part of deterrence is both -- some aspects to

1 deterrence -- convincing someone that the benefit that  
2 they will gain doesn't justify the cost, convincing the  
3 actor that they just won't succeed, or convincing the  
4 actor that, "Even if you were to do this, and even if you  
5 were to succeed, what we'll bring back against you in  
6 response to this just doesn't merit you doing this. You  
7 really ought to think hard and fast before you really do  
8 this." And I have said this multiple times publicly  
9 before. The challenge we have right now is, I think, for  
10 a variety of reasons, some -- not all -- some actors have  
11 not yet come to the conclusion that there's a significant  
12 price to pay for some pretty aggressive actions on their  
13 part in the cyber arena.

14 Senator Nelson: Well, I'd like to follow with you, in  
15 a classified setting --

16 Admiral Rogers: Sir.

17 Senator Nelson: -- how we might respond to some of  
18 those actors.

19 Admiral Rogers: Sir.

20 Senator Nelson: In the private sector, do we have the  
21 cooperation that we need to tackle these encryption  
22 challenges?

23 Admiral Rogers: At an operational level, my  
24 observation -- because this is much bigger than just Cyber  
25 Command or NSA -- my answer would be no, in the sense that

1 -- my sense, as I look at this problem set, I see multiple  
2 parties spending a lot of time talking about what they  
3 can't do or what can't be done. And I wish we spent more  
4 time thinking about, Well, what could we do, what is in  
5 the realm of other possible? Even as I acknowledge I  
6 think there's multiple parts to this conversation. What  
7 can we do is not necessarily the same thing as what should  
8 we do. And those are two very important parts of this  
9 conversations that I think we need to have.

10 Senator Nelson: And the encryption thing does trouble  
11 all of us.

12 Admiral Rogers: Sir.

13 Senator Nelson: Aside from encryption, what other  
14 technology trends are shaping the way that the Department  
15 does business?

16 Admiral Rogers: It -- from a cyber perspective?

17 Senator Nelson: Yes.

18 Admiral Rogers: We're very much interested in  
19 artificial intelligence, machine learning. How can we do  
20 cyber at scale, at speed? Because if we're just going to  
21 make this a largely human capital approach to doing  
22 business, that is a losing strategy. It will be both  
23 incredibly resource-intensive, and it will be very slow.  
24 So, I'd say that is a big area of focus for us. In  
25 addition, we're constantly reaching out -- DIUX, the

1 capability that's been created out in Silicon Valley as  
2 well as Boston, U.S. Cyber Command has a separate but  
3 related -- that teams with DIUX to try to harness  
4 partnerships in the private sector.

5 Overall, I'd say good. But, as the Chairman  
6 highlighted, every once in a while, you just run into a  
7 situation where you go, "Can't we just step back, sit  
8 down, and talk to each other rather than, you know, these  
9 arbitrary, 'Hey, you can't do this, you can't do that, we  
10 won't do this, we won't do that'?" Even as I acknowledge  
11 there are different perspectives out there, I have no  
12 issue with that at all. I certainly understand that.

13 Senator Nelson: Thank you, Mr. Chairman.

14 Chairman McCain: Senator Lee.

15 Senator Lee: Thank you, Mr. Chairman.

16 Thanks, to both of you, for being here. I also  
17 appreciate your commitment to protecting the rights that  
18 we hold dear as Americans, and our security.

19 This issue of encryption cuts right to the heart of a  
20 lot of things. It cuts right to the heart of the nature  
21 of the relationship between the American people and their  
22 national government, and to the heart of a number of  
23 features in the Constitution, including responsibilities  
24 of the Federal Government to safeguard the people and also  
25 to safeguard their rights.

1 I believe it's an issue that Congress and the executive  
2 branch have to approach with a great deal of prudence,  
3 recognizing that we can't view it exclusively either as a  
4 national security issue, on the one hand, or as a privacy  
5 issue, on the other hand. We have to view it  
6 holistically, understanding that we've got to find a  
7 resolution to this that respects all the interests at  
8 stake.

9 Admiral Rogers, I'd like to start with you. On August  
10 17th, the Washington Post reported that a cache of  
11 commercial software flaws that had been gathered by NSA  
12 officials was mysteriously released, causing concerns both  
13 for government security and also for the security and the  
14 integrity of those companies who I believe had not been  
15 notified by the NSA of the flaws discovered in their  
16 systems. So, can you walk through this process with us  
17 that the NSA uses to determine --

18 Admiral Rogers: Vulnerability?

19 Senator Lee: Yeah. Well, to determine when, whether,  
20 to what extent you should notify a private company of a  
21 security vulnerability that you've discovered, and whether  
22 NSA will continue to withhold such information from those  
23 companies when you're holding those and there are some  
24 clear concerns about the security of your own systems.

25 Admiral Rogers: So, there's a vulnerability evaluation

1 process, interagency, that was started in 2014, that we  
2 continue to be a part of, whereas NSA and other entities,  
3 not just us, become aware of, you know, zero-day  
4 vulnerability, so to speak, those vulnerabilities that we  
5 don't think are -- others are aware that haven't been  
6 patched or addressed, that we raise those through an  
7 interagency process, where we assess what's the impact of  
8 disclosing or not disclosing. I have said publicly  
9 before, I think, over the last few years, overall -- I  
10 think our overall disclosure rate has been 93 percent or  
11 so of the total number of vulnerabilities using this  
12 process since 2014. And we continue to use that process.

13 Senator Lee: Okay. Okay. So, you do that on a case-  
14 by-case basis --

15 Admiral Rogers: Yes, sir.

16 Senator Lee: -- depending on the totality of the  
17 circumstances.

18 Has there been an instance in which a U.S. company has  
19 suffered a security breach because of a cyber  
20 vulnerability that you were aware of that you -- that NSA  
21 had previously identified but --

22 Admiral Rogers: I can't say totality of knowledge,  
23 sir. I don't know totality. I apologize.

24 Senator Lee: Okay. No, it's understandable.

25 On Sunday, just this past Sunday, the Wall Street

1 Journal published a report on the methods of ISIS, the  
2 methods that ISIS is using, in which there were some  
3 experts who concluded that low-tech communications,  
4 including things like face-to-face conversations,  
5 handwritten notes, and sometimes the use of burner phones,  
6 have proven to be just as much of a problem for Western  
7 intelligence officials as the use of high-end encryption  
8 by our adversaries.

9 Mr. Secretary, I was wondering if I could get your  
10 sense on this. Are the defense and intelligence  
11 communities investing enough into human intelligence and  
12 other activities to address low-tech terror methods, like  
13 those leading up to the Paris attacks? And if we  
14 continue, I -- a related question to that is, If we  
15 continue focusing on combating highly sophisticated  
16 encryption technology, do we expect to see a corresponding  
17 shift into these lower-tech alternatives?

18 Mr. Lettre: Senator, you're -- you've put your finger  
19 on a really important point, which is the need for a  
20 really diverse set of intelligence collection capabilities  
21 and disciplines. Capabilities that go after the high end,  
22 using the best of our technology available, but also  
23 capabilities that draw upon individual case officers, area  
24 expertise, language expertise, and presence on the ground  
25 in a lot of places around the world, where we can, in a

1 very granular way, pick up what's going on and identify  
2 threat actors who, as you noted, may be using relatively  
3 unsophisticated mechanisms for planning and plotting  
4 attacks against the U.S. homeland and our allies. So,  
5 with regard to the aspect of your question around human  
6 intelligence, we have been making some investments, over  
7 the last several years, to continue to improve the  
8 effectiveness and capacity of defense-related human  
9 intelligence, working closely with CIA. And I think that  
10 that is a very important set of investments to be making.

11 Admiral Rogers: Senator, could I add one comment?

12 Senator Lee: Sure.

13 Admiral Rogers: That would be okay?

14 I think what that article highlights is the fact that  
15 we are watching ISIL use a multi-tiered strategy for how  
16 they convey information and insight that runs the entire  
17 gamut. And so, I think, for us, as intelligence  
18 professionals, we've got to come up with a strategy and a  
19 set of capabilities that are capable of working that  
20 spectrum. It can't be we just spend all our money focused  
21 on one thing. I don't think that's a winning strategy for  
22 us, if that makes sense.

23 Senator Lee: Understood.

24 I've got a couple of other questions, but my time's  
25 expired, so I'll submit those in writing.

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

Thank you very much.

[The information referred to follows:]

[COMMITTEE INSERT]

1 Chairman McCain: Senator Heinrich.

2 Senator Heinrich: Thank you, Mr. Chair.

3 Admiral Rogers, I want to continue along that line of  
4 questioning. And recently there was a worldwide survey,  
5 actually, of encryption products, looked at 865 hardware  
6 and software commercial encryption products that are  
7 available worldwide. And about a third of those were  
8 developed in the U.S.; two-thirds were developed overseas.  
9 You know, it begs the question, If Congress were to act on  
10 this issue, if Congress were to compel some sort of built-  
11 in backdoor to those kinds of products, would that in any  
12 way effectively limit access to strong encryption projects  
13 to our enemies, to foreign terrorist groups? So long as  
14 they're widely available on the Internet?

15 Admiral Rogers: So, I think, clearly, any structure,  
16 any approach that we come up with here with respect to  
17 encryption has to recognize that there is an international  
18 dimension to this, that encryption doesn't recognize these  
19 arbitrary boundaries on the globe that we have drawn, in  
20 the form of borders of nation-states. I don't know what  
21 the answer is, but I certainly acknowledge we have to  
22 think more broadly than just one particular market, so to  
23 speak.

24 Senator Heinrich: Given how easy it is to just  
25 download an app onto your smartphone to do end-to-end

1 encryption of texting and other communications, does it --  
2 and getting to, really, Senator Lee's question -- does it  
3 beg the question of whether or not we've become overly  
4 reliant on signals intelligence, generally? Are we  
5 investing enough in human intelligence?

6 Admiral Rogers: I'll leave that up to the Under  
7 Secretary. I'm a --

8 Senator Heinrich: I know it's dangerous question for  
9 someone in your position, but --

10 Secretary?

11 Mr. Lettre: Senator, the short answer is, we do need  
12 to be investing in a range of capabilities, including the  
13 human intelligence capabilities. As to the point about  
14 individuals being able to download an app onto their  
15 mobile phones and smartphones that can avoid law  
16 enforcement or national security coverage, it really just  
17 underscores the imperative for a really rich and diverse  
18 set of conversations to be going on between government and  
19 all players across the technology sector. Each company  
20 has a different business model, which may or may not  
21 implement end-to-end encryption in a ubiquitous way, and  
22 we need to be looking for solutions on a case-by-case  
23 basis that allow us to preserve our values, including the  
24 ability to conduct law enforcement and national security  
25 protective operations in service of the Nation.

1           Senator Heinrich: You know, one of the issues that was  
2           raised earlier is this idea of identifying vulnerabilities  
3           that may exist in software, in operating systems, in  
4           hardware. Obviously, when there are those  
5           vulnerabilities, it means that people who work for the  
6           U.S. Government, as well as private citizens, have data  
7           potentially exposed to nefarious actors. Has the  
8           administration ever considered some sort of reward  
9           structure, incentive structure for those sorts of  
10          vulnerabilities to be identified and, therefore,  
11          identified to companies so that they can plug those holes  
12          as they come up?

13          Admiral Rogers: I can't speak for the administration  
14          as a whole, but we have done this twice now within the  
15          Department of Defense, you could argue, in the Bug Bounty  
16          Program, where we specifically have tried to incentivize  
17          the discovery and sharing of vulnerabilities, both to help  
18          the Department as well as to help the commercial sector in  
19          trying to address them. That's something that we've been  
20          doing.

21          Senator Heinrich: Have you found that to be a -- an  
22          effective strategy?

23          Admiral Rogers: Yes, sir. And, in fact, you'll see us  
24          -- in the coming months, we're looking at the next  
25          iteration of the program, as well. This is something we

1 want to continue.

2 Senator Heinrich: Do you think that's something we  
3 should be looking at as a more whole-of-government  
4 approach, as well?

5 Admiral Rogers: I would only say, our experience has  
6 been a positive one, and I would fully expect that it  
7 would turn to be positive for others. The scale is --

8 Senator Heinrich: I know with my conversations with  
9 the technology sector, that's something that's come up --

10 Admiral Rogers: Right.

11 Senator Heinrich: -- consistently over time.

12 Thank you both.

13 Chairman McCain: Senator Sullivan.

14 Senator Sullivan: Thank you, Mr. Chairman.

15 Thank you, gentlemen, for the testimony today.

16 Admiral Rogers, I just want to get -- and I know you've  
17 been talking about this in a more broad sense, but what do  
18 you see as the three top threats that U.S. Cyber Command  
19 or the NSA have to plan or defend against? Top three.  
20 And it can be a country or it can be an issue. When  
21 you're going to bed at night, what are the top three that  
22 you're --

23 Admiral Rogers: So, broadly, as I look out, number one  
24 is just the day-to-day defense of the DODIN. I look at  
25 DOD. We are a massive Department with a global laydown

1 and a network infrastructure that was built in a different  
2 time and a different place, in which redundancy,  
3 resiliency, and defensibility were not core design  
4 characteristics. And so, my challenge at the Cyber  
5 Command side is, I've got to defend an imperfect  
6 infrastructure and give us the time to make the  
7 investments to build something better. So, that's  
8 challenge number one. I'm always thinking to myself, what  
9 are the vulnerabilities out there that I don't recognize  
10 yet that someone's exploiting?

11 Number two would probably be -- I worry about -- most  
12 penetrations in networks to date have largely been about  
13 extracting information -- extracting, pulling the data --  
14 whether it's to generate intelligence insights, whether  
15 it's to generate battlefield insights, whether it's to  
16 potentially attempt to manipulate outcomes. What happens  
17 when it's no longer just about data extraction, but it's  
18 about data manipulation, and now data integrity becomes  
19 called into question? As a military commander, if I can't  
20 believe the tactical picture that I am seeing, that I'm  
21 using to make decisions, that are designed to drive down  
22 the risk and help me achieve the mission, if what I'm  
23 seeing is a false representation and, in fact, the choices  
24 I'm making are increasing the risk and, in fact, are not  
25 having positive outcomes -- data integrity, data

1 manipulation really concerns me. That's a whole different  
2 kettle of fish.

3 And then the third one, probably, What happens when  
4 nonstate actors decide that the Internet is not just a  
5 forum to coordinate, to raise money, to spread ideology,  
6 but instead offers the opportunity to act as a weapon  
7 system, to employ capability on a global scale?

8 Senator Sullivan: So, let me ask about that last one,  
9 because I think one of the things that we continually  
10 hear, in terms of our cyber strategy and how it -- and how  
11 the -- this domain differs in so many other domains -- is  
12 that the attacks, when they occur on us, seem to come, in  
13 some cases, without much cost. So, we're getting hit from  
14 all different angles, and we're not sure where or how, and  
15 you can't do a symmetrical smackdown, maybe. But, how do  
16 we -- how do we raise the costs for adversaries who are  
17 attacking us in this domain? Or how do we signal that  
18 we're going to do it? Obviously, a lot of it -- if we're  
19 signaling, we have to have credibility. But, how do we  
20 raise the cost? Do you think we do need to raise the  
21 cost? Do you think, in this domain, that our adversaries  
22 or potential adversaries think that they can take action  
23 and kind of get away with it because we're not going to  
24 respond? Do we need to be more aggressive in signaling  
25 how we're going to respond, and then respond?

1 Admiral Rogers: And I think we need to show adversary  
2 we have capability, we have intent, and we have the will  
3 to employ it, within a legal framework --

4 Senator Sullivan: Have we done that, though, much?

5 Admiral Rogers: We have -- as I've said, we've done  
6 it. The Sony piece, I would argue. You could also argue,  
7 in the areas of hostilities -- Syria, Iraq, Afghanistan --  
8 we're doing some good things every day that clearly I  
9 think the opponent understands that we're applying this  
10 capability against them. We've publicly acknowledged that  
11 we are doing that. I think, in part, that idea of  
12 publicly acknowledging the fact that we were using cyber  
13 as a capability to counter ISIL was not just to signal  
14 ISIL, but was also to make sure others are aware that the  
15 Department of Defense is investing in these capabilities,  
16 we are prepared to employ them, within a legal, lawful  
17 framework.

18 Senator Sullivan: Do you think we're sending that  
19 signal to state actors in the cyberspace?

20 Admiral Rogers: I certainly hope so, sir.

21 Senator Sullivan: Well, do you think we are? I don't  
22 know what --

23 Admiral Rogers: I think it --

24 Senator Sullivan: You're the -- you're in charge,  
25 right? So, "hope" makes me a little worry. What you

1 think --

2 Admiral Rogers: It varies by the actor. Honestly. It  
3 varies by the actor.

4 Senator Sullivan: Do the Iranians fear that we could  
5 retaliate against them if they take some kind of cyber  
6 action?

7 Admiral Rogers: Yes. My sense is, the Iranians have a  
8 sense for a capability. And I'm -- apologize, I can't get  
9 into a lot of specifics, but my sense is, they have  
10 awareness of capability, and they've seen us use it.

11 Senator Sullivan: Let me ask this one final question.  
12 It seems to me, kind of longer term, one of the biggest  
13 strategic advantages we have in this domain is our youth  
14 and their capabilities, which far exceed, probably,  
15 everybody in this room, given how smart they are in this  
16 space and how they've just naturally grown up with it.  
17 What are we doing to make sure to try to recruit younger  
18 Americans to, you know, be on the right side of the issue,  
19 to come serve their country in a really critical area,  
20 where they, in many ways, have unique skillsets that a lot  
21 of us -- no offense to my colleagues around the dais here  
22 -- that a lot of us don't have?

23 Admiral Rogers: Yes, sir. On the NSA side, I'll just  
24 highlight a couple of examples. We have a conscious  
25 effort that we've been doing for several years now. We do

1 high school and junior high school cyber camps that we  
2 partner with a variety of institutions across the United  
3 States. We have cyber acquisition -- or cyber academic  
4 excellence and academic research excellence relationships  
5 with over 200 universities on the NSA side across the  
6 United States, because we realize much of the workforce  
7 that we're looking to gain in the future is going to come  
8 from these pools. And so, there's something to be gain,  
9 we believe, by interacting early with them, and, more  
10 broadly, for the Nation as a whole, helping to encourage  
11 the acquisition of these skills, this knowledge, in a way  
12 that just wasn't necessarily the case in the past.

13 Senator Sullivan: Thank you.

14 Thank you, Mr. Chairman.

15 Chairman McCain: Senator Manchin.

16 Senator Manchin: Thank you, Mr. Chairman.

17 And thank both of you all for being here.

18 Admiral Rogers: Sir.

19 Senator Manchin: And along the line of questioning  
20 there, for those of us who grew up in the not-Internet  
21 Age, if you look around at some of us here in the audience  
22 and some of us on this -- and now all this coming to  
23 fruition, it's quite confusing, quite troubling, quite  
24 concerning. With all that being said, you know, we have  
25 concern over our food supply, our energy supply. The

1 average person in America right now is concerned over,  
2 whether they have children or grandchildren, cyber  
3 bullying, everything that goes on with the Internet. We  
4 see the rise of terrorist -- the great equalizer is the  
5 Internet for them. They don't have an air force, they  
6 don't have a navy. They have nothing more than the will  
7 to do us harm or wreak havoc around the world.

8 With all that being -- going on, the question I would  
9 like to ask best is, In a perfect world, without the  
10 politics involved, not being -- trying -- being  
11 politically correct, what can we, as Senators sitting on  
12 this committee or in this body or in Congress, 535 of us,  
13 concentrate and do to allow you to streamline this to make  
14 this work? It looks to me like you're going to take a  
15 covey of volunteers around the country that are smart and  
16 bright, to recruit them, but also, if people are out there  
17 hacking us continuously, are they able to intercede? Are  
18 they able to see what's going on? Are they able to report  
19 -- is there some way of communication that the average  
20 person say, "Listen, I've seen some activity going on here  
21 that I think is going to be detrimental to us, think you  
22 ought to know about." You all have a -- an agency -- I  
23 mean, a way that you can collect this information? And  
24 what can we do to help to streamline this, to correct  
25 this, so it doesn't get so convoluted that something falls

1 through the cracks?

2 Whoever wants to take that one, you can --

3 Mr. Lettre: Senator, I'll take a first crack at it.

4 Really, the most important thing, I think, that we can all  
5 do -- and this committee and you all, as members, are  
6 incredibly powerfully well suited and seated to be able to  
7 do this -- is to have that dialogue, catalyze that  
8 dialogue with the public, with civic leaders, with  
9 industry leaders, about the shared nature of this  
10 challenge, both the cybersecurity challenge and the  
11 hacking that we all face across -- from the individual to  
12 companies and governments, and the acute threat from --  
13 ongoing threat from terrorism, and the need to put our  
14 best foot forward, in terms of countering violent  
15 extremist messaging, countering their ability to recruit  
16 and persuade over the Internet. And so, that --

17 Senator Manchin: I think --

18 Mr. Lettre: -- that dialogue with leaders to really  
19 impress upon corporate and civic leaders the need to have  
20 -- view that as a shared problem and to really look for  
21 solutions with us.

22 Senator Manchin: Well, the question I'm asking, I  
23 think, to both of you all, is that -- I mean, if you're  
24 looking at us as a -- everybody says lack of money, it's  
25 always a money situation, to a certain extent, or is it a

1 lack of, basically, siloing to where everyone's protecting  
2 their own territory? Is there a way that we can break  
3 through, that, if you're going to be that agency, there  
4 has to be one gathering point and, basically, one  
5 dispensing point. And I'm understanding that some of our  
6 agencies aren't talking to each other. We have the  
7 situation to where we don't have the private sector  
8 cooperating -- San Bernardino, Apple, and all that, that  
9 comes to mind. This can't happen. If that's the great  
10 equalizer, and we have people that have nothing else more  
11 than the will to do us harm, we have to have the will to  
12 protect greater than the will to do harm.

13 Admiral, I'm looking for just a way to help.

14 Admiral Rogers: So, Senator, I don't disagree with  
15 many of the statements you're making. This is my  
16 takeaway, having done this for a while now. Using the  
17 same structures and the same processes and expecting  
18 different outcomes probably is not going to get us --

19 Senator Manchin: We understand that definition.

20 Admiral Rogers: -- where we want to be. So, I think  
21 the challenge, particularly as we're looking in the  
22 future, is, Can we take the opportunity to step back and  
23 ask ourselves, "Hey, what do we need to be doing  
24 differently?"

25 The other thing, I think, particular as Senators, as

1 among the leaders of our Nation, these are serious, hard  
2 issues, with a wide variety of perspectives, and we have  
3 got to get beyond this simplistic vilification of each  
4 other to roll up our sleeves and figure out, How are we  
5 going to make this work? Realizing that there's multiple  
6 perspectives and a lot of different aspects of this that  
7 have to come to the fore.

8 Senator Manchin: You know, I tell -- I speak to  
9 children and -- much as I possibly can. I would -- and I  
10 tell them, I says, I don't think -- nowhere in the world  
11 is there a military might that can challenge us. We have  
12 the greatest military in the world. The economy -- our  
13 economy is greater than anyone in the world, almost double  
14 the closest -- of China. I'm not worried about a military  
15 or an economic takeover of the United States of America.  
16 I worry every day about the cyber -- breaking down the  
17 cybersecurity, how they hack and whack at us and,  
18 basically, come at us different ways. And if we're not  
19 defending that, if we're not giving you the tools, and if  
20 we're playing politics, being Democrat and Republican and  
21 who's politically correct -- this is not a time to do  
22 that.

23 I think there's a group of us here that would love to  
24 step out and say, "Okay, how do we streamline this? How  
25 do we make sure that someone says, 'We do this, or we

1 don't do this, or we go in this direction'?" That's what  
2 we're looking for. And hopefully you know that we're here  
3 to help there.

4 Admiral Rogers: Yes, sir.

5 Senator Manchin: Thank you.

6 Chairman McCain: Senator Shaheen.

7 Senator Shaheen: Thank you, Mr. Chairman.

8 And thank you both for being here today.

9 I want to follow up a little bit on Senator Manchin's  
10 question, which was really referred back, I think, to  
11 Senator McCain and the Twitter example that you used  
12 earlier.

13 So, how do we get some of those private-sector  
14 companies to recognize that this a shared challenge and  
15 that we've got to work together? Do we need more  
16 legislation to address that? And this is really a policy  
17 question for you, Secretary. So, is it that, or is it  
18 meeting with folks? What do you think we need?

19 Mr. Lettre: Senator, our view, at this point in the  
20 dialogue and debate, is that legislation that forced or  
21 required a regulatory solution is not preferred, at this  
22 point. And what we have found is that, on a case-by-case  
23 basis, when leaders from the executive branch have been  
24 able to have a very effective, quiet dialogue with leaders  
25 in industry, that the nature of the conversation starts to

1 shift in a couple of ways. One is, you know, industry and  
2 government, for decades, have worked together very proudly  
3 on projects that protect the Nation. And so, reminding  
4 ourselves of that rich history, I think, starts to put the  
5 conversation into a dialogue around solutions rather than  
6 being at odds with each other in an antagonistic way. If,  
7 on the government side, we're able to communicate the  
8 problems we're trying to solve and ask for industry's best  
9 expertise and wisdom about the solutions that might be  
10 brought to bear that we haven't even thought about yet,  
11 often we find that we are able to come up with solutions  
12 that meet our law enforcement and national security needs.

13 The second thing that I think is --

14 Senator Shaheen: Well, let me just --

15 Mr. Lettre: -- that we --

16 Senator Shaheen: -- I'm sorry to interrupt, but has  
17 that worked with Twitter, in terms of the willingness of  
18 Twitter to allow us to scrub some of the information that  
19 they have?

20 Mr. Lettre: As was mentioned earlier, to the best of  
21 my knowledge, Twitter's position hasn't changed on its  
22 level of cooperation with the U.S. intelligence community,  
23 so far.

24 Senator Shaheen: And we were not very successful with  
25 Apple, either. Is that correct?

1 Mr. Lettre: That's right, yeah.

2 Senator Shaheen: So, there are limits. Certainly,  
3 there are limits to that kind of a strategy. I appreciate  
4 what you're saying. I mean, I would -- I have a -- always  
5 rather try and sit down and resolve the situation rather  
6 than pass legislation, but right now we've had mixed  
7 reviews of the opportunity to work collaboratively with  
8 the private sector to address this issue.

9 Mr. Lettre: Yeah, that's absolutely fair to say. Now,  
10 the industry and the private sector is very diverse.  
11 Businesses --

12 Senator Shaheen: Sure.

13 Mr. Lettre: -- have different business models, which  
14 leave them in different positions, as far as their ability  
15 or willingness to work closely with government on working  
16 our way through some of these law enforcement questions.  
17 So, it -- a case-by-case approach, I think, is what is  
18 absolutely needed. But, as you pointed out, we are not  
19 successful in every case.

20 Senator Shaheen: I had the opportunity, earlier this  
21 year, to visit Estonia, which, as we know, was the first  
22 state subject to a massive cyberattack from Russia. Are  
23 there lessons to be learned from examples like Estonia who  
24 have experienced this, or from other countries or  
25 businesses?

1 Admiral Rogers, are there lessons that we should be  
2 taking from what's happened in other places?

3 Admiral Rogers: So, it's not by chance that I've been  
4 to Estonia twice in the past year. Again, I'm not going  
5 to get into specifics, but we have talked about creating a  
6 relationship to try to build on it. Although one comment  
7 I make to my Estonian teammates also is, what works  
8 necessarily in your construct may not --

9 Senator Shaheen: Sure.

10 Admiral Rogers: -- necessarily scale directly to a  
11 nation of 350- -- you know, 335 million and the largest  
12 economy in the world. But, there are perhaps some things  
13 that we can take away from this. Because you have to  
14 admire -- they sat down and decided this was a national  
15 imperative for them, and they consciously sat down and  
16 asked themselves, So, what do we need to do to get where  
17 we want to be? And then, how can the government help to  
18 be a primary driver in this? Not the only focus, but how  
19 can we harness the power of the government and their  
20 structure to help drive that? And that aspect of it is  
21 very impressive, to me.

22 Senator Shaheen: I would agree with that. I was very  
23 impressed with what I heard. But, to follow up on what  
24 you're saying, do you think we've reached the point where  
25 we believe that this is a national imperative for the

1 United States?

2 Admiral Rogers: Intellectually, my sense is, most  
3 people intuitively realize that, but then translating that  
4 into a series of specific actions to drive broader change  
5 than we have done, I think that is still the rub, if you  
6 will.

7 Senator Shaheen: Thank you.

8 Thank you, Mr. Chairman.

9 Chairman McCain: Senator Cruz.

10 Senator Cruz: Thank you, Mr. Chairman.

11 Mr. Secretary, Admiral, thank you for your service.

12 Thank you for joining us today on this vital topic before  
13 this committee.

14 Admiral Rogers, during your testimony to this committee  
15 in April, you indicated that the Department of Defense was  
16 making significant progress towards establishing 133 Cyber  
17 Mission Force teams with plans to be fully operational by  
18 the end of fiscal year 2018. In my home State of Texas,  
19 I'm very proud of the contributions of the Air Force Cyber  
20 Command. I'm glad to see that the Air Force is taking  
21 advantage of the unique synergies between the academy,  
22 industry, and the military which exist in San Antonio.  
23 The combined efforts of the Air National Guard and the  
24 Active Duty Forces at Lackland have played, and will  
25 continue to play, an integral role in modern cyber

1 warfare. And I thank them for their hard work, and you  
2 for your leadership to ensure that they have the right  
3 tools they need to train, to fight, and to win.

4 Admiral Rogers, would you provide an update on the  
5 Cyber Mission Force and detail specific shortfalls that  
6 merit congressional assistance?

7 Admiral Rogers: So, the Cyber Mission Force, 6,187  
8 individuals and 133 teams focused on three missions,  
9 providing capability to provide combatant commanders, if  
10 you will, with offensive capability, providing defensive  
11 capability to defend the DODIN, if you will, the DOD  
12 network structure, also the third mission set for us,  
13 providing capability to help defend critical U.S.  
14 infrastructure against significant acts of cyber  
15 consequence, if you will. Three primary mission sets,  
16 those 133 teams, if you will, break down into those three  
17 different missions.

18 The first goal we had was IOC of the 133 teams by 30  
19 September of 2016. That's 3 weeks from now -- or 2 weeks  
20 or so from now. We will be IOC by 30 September 2016 of  
21 all teams. And I would compliment the services, because  
22 this is one where, quite frankly, I haven't been the  
23 nicest individual, at times, about, what don't we  
24 understand about -- this is a goal and a standard, and we  
25 are going to meet this. So, we're on track to do that.

1       The next major milestone, if you will, in the fourth  
2 generation, is to be at full operational capability by 30  
3 September 2018, because our experience is that it takes  
4 about 2 years to get a team, from the time we stand it up  
5 til it's fully mission capable, so the teams we're  
6 finishing standing up this month in IOC, we expect it'll  
7 take us 2 years to get them to full operational  
8 capability.

9       The biggest challenges meet a continue -- we continue  
10 to learn insights about tools on the cyber defensive side  
11 that we need to continue to deploy more broadly. I'm  
12 trying to use a best-of-breed approach to this across the  
13 Department, whereas we generate insights from capabilities  
14 that the individual services have -- NSA, DISA, other  
15 elements -- let's pick the best of breed, and let's apply  
16 it more broadly. Let's not waste money, everybody trying  
17 to do their own thing, here.

18       Investment in the persistent training environment, our  
19 ability to actually simulate, in garrison, the networks  
20 that we're going to defend, the networks that we're going  
21 to operate on. That's fundamental to the future for us.  
22 We just cannot afford a model, where we do these major  
23 exercises, we try to bring everybody together. It's just  
24 a cost-intensive approach to doing business. It's a part  
25 of our strategy, but it shouldn't be the fundamental

1 backbone.

2 Cyber situational awareness is another area where I  
3 would argue we have got to be able to visualize this  
4 battlespace. And right now, we just don't do that well.  
5 I have prioritized it at a lower level. I'm the first to  
6 acknowledge that. We've had to identify where can we take  
7 risk, so I've tended to prioritize it lower. But, it's an  
8 area where I remain concerned from a -- we need to  
9 increase the level of investment. We're taking too much  
10 risk.

11 Those are probably the -- I don't want to give you a  
12 long answer, because I know you have limited time, Senator  
13 -- those would probably be the three biggest areas that I  
14 would argue we need to keep focused on, keep investing on.

15 Senator Cruz: Okay. Thank you, Admiral.

16 Let me shift to a different topic. An NBC news article  
17 this week claims that, despite evidence that Russia is  
18 behind a number of cyber intrusions into American  
19 networks, that the administration failed to respond  
20 because it determined that we need Russia's help in Syria.  
21 If true, the Obama administration will have effectively  
22 ignored the threats from an adversary, that it is actively  
23 trying to influence the election process and will set a  
24 terrible precedent for our country, going forward.

25 Mr. Secretary, are these reports true? And is this, in

1 fact, what the administration's done?

2 Mr. Lettre: I'm not aware of the details of that  
3 particular NBC story, Senator, but I'm not aware of any  
4 linkage of these issues that I've seen in the policy  
5 discussions. The incidents that you've described around  
6 the apparent hacking related to our electoral systems is  
7 under an aggressive FBI investigation so that the U.S.  
8 Government can compose its own conclusions about what has  
9 occurred there and what are the appropriate actions to  
10 take in response. To the discussion that the committee  
11 has been having this morning around cyber deterrence, it  
12 will be very important to look at the facts around that  
13 investigation and the conclusions from it in order to  
14 inform policy choices about what kind of acts to take in  
15 response.

16 Senator Cruz: Very well.

17 Thank you.

18 Chairman McCain: Senator Blumenthal.

19 Senator Blumenthal: Thanks, Mr. Chairman.

20 Thank you for -- both for your service and the  
21 excellent contribution that you're making to our national  
22 defense.

23 I want to return to the Chairman's questions about our  
24 electoral system. Isn't there a pretty powerful argument  
25 that our systems of elections and voting ought to be

1 declared critical infrastructure?

2 Mr. Lettre: Senator, that -- that's an important  
3 question. I think, when we look at critical  
4 infrastructure across the country, we do need to consider  
5 the possibility of attacks on infrastructure causing  
6 significant consequences to the U.S. And if there were  
7 scenarios where we could envision attacks having  
8 significant consequences in our electrical -- electoral  
9 context, we really do need to consider that.

10 Senator Blumenthal: Well, certainly we've envisioned  
11 those potential consequences.

12 Admiral, your response to the Chairman's question was,  
13 in part, that this electoral system is -- I think you used  
14 the word "disparate," by which I took it to mean  
15 decentralized; "disparate" meaning divided and localized  
16 --

17 Admiral Rogers: Yes, sir.

18 Senator Blumenthal: -- which is true. Every State has  
19 its own system. But, as you well know, in our  
20 presidential elections, the electoral college is the  
21 critical decision maker, which results from elective  
22 systems within States. And, of course, elections have  
23 consequences at the State and local level, as well, and  
24 now many are driven or directed by some kind of computer  
25 collection of information, so they are vulnerable, maybe

1 not at the ballot box, but at some point in the chain of  
2 collecting and assimilating that information. Isn't that  
3 troubling to you? And I don't know the circumstance of  
4 Arizona. You're not familiar with the circumstance of  
5 Connecticut, but --

6 Admiral Rogers: Right.

7 Senator Blumenthal: -- this is a common thread in our  
8 elective system. And we've seen, from some of these  
9 hacks, that they can have very severe impacts on the --  
10 these systems, and they are largely unprotected right now.

11 Admiral Rogers: I think it raises a broader question  
12 of, What is truly critical in the cyber world? You know,  
13 we've tended to think -- I think, my sense -- we've tended  
14 to think along very traditional industrial, in many ways,  
15 you know, kinds of lines. And one of the things, I think,  
16 that the events in the last few years are highlighting to  
17 us is that, for example, we need to think about data in a  
18 whole different way. And what are the implications from a  
19 security and a critical infrastructure --

20 Chairman McCain: But, Admiral, wouldn't the selection  
21 of our leaders -- of our system of government be -- there  
22 should be no discussion about that.

23 Admiral Rogers: So, Senator, my --

24 Chairman McCain: If you attack that, and succeed in  
25 destroying that, you've destroyed democracy.

1 Admiral Rogers: So --

2 Chairman McCain: Why are we equivocating, here, about  
3 this? I'm sorry to interrupt.

4 Senator Blumenthal: No, I --

5 Chairman McCain: -- Senator Blumenthal.

6 Senator Blumenthal: Mr. Chairman, you took the words,  
7 much more eloquently, out of my mouth. I think there is  
8 not only a powerful argument, it's virtually  
9 incontrovertible.

10 And I understand that you're approaching it from a more  
11 abstract standpoint. And I don't mean to interrupt,  
12 because I'm here to listen to you, but I would hope that  
13 there would be a move to designate these systems as  
14 critical infrastructure. And why don't you -- I know you  
15 were remarking on the --

16 Admiral Rogers: Yes, sir.

17 Senator Blumenthal: -- nature of data.

18 Admiral Rogers: So, my only point is, if you look at  
19 critical infrastructure, from a data perspective, and you  
20 look at -- So, what are the key data-driven decisions that  
21 tend to shape us of a -- as a Nation? -- you come to a  
22 very different conclusion about an election that --  
23 structure -- for example, that if your perspective was,  
24 "Well, critical infrastructure, to us, is primary  
25 industry" -- that that's my only point to you, is, this

1 leads us, I think, to a different set of conclusions as to  
2 what is truly critical, here. And an election system is a  
3 good example of that.

4 Senator Blumenthal: Well, my time has expired, but I  
5 think that we really need a national consensus that our  
6 electoral system, our system of choosing our leaders, as  
7 the Chairman has said very well -- our system of choosing  
8 leaders at every level, not just the national level, but  
9 State government, State legislators -- all of these  
10 systems are going to be increasingly involving the  
11 collection of -- you refer to it as "data" -- the data are  
12 votes. The votes are individual citizens deciding who  
13 their leadership is going to be, which is going to  
14 determine who sits in the chair you occupy right now. And  
15 these chairs here. And who makes these critical  
16 decisions. Nothing is more fundamental -- our financial  
17 system, our utilities, our system of healthcare, all are  
18 critical infrastructure. And I think our system of  
19 electing and choosing leaders is no less so.

20 Thank you very much.

21 Chairman McCain: Senator Ernst.

22 Senator Ernst: Thank you, Mr. Chair.

23 Gentlemen, thank you very much for coming in today and  
24 talking about cybersecurity and its impact on our national  
25 security.

1 I'd like to address some situations from the National  
2 Guard perspective. I'm a former soldier in the Iowa  
3 National Guard, and I have been tracking the increasing  
4 cyber capabilities that both the Army and the Air National  
5 Guard are bringing to the table, even in my own home State  
6 of Iowa. But, unfortunately, it appears that the DOD has  
7 not been tracking this as closely as I have.

8 A report from the GAO last week stated that, quote,  
9 "DOD does not have visibility of all National Guard unit  
10 cyber capabilities, because the Department has not  
11 maintained a database that identifies the National Guard  
12 units' cyber-related emergency response capabilities, as  
13 required by law," end quote.

14 This is a little bit alarming to me, because, in the  
15 National Guard, we do have some tremendous capabilities,  
16 and we're able to poll a number of those private-sector  
17 cyber warriors into the Guard. That's their part-time job  
18 and full-time job. So, they are very talented, and we  
19 want to see that they are being used to the fullest of  
20 their capabilities.

21 Admiral, how close is the DOD to having a database of  
22 all of the National Guard cyber capabilities required by  
23 law?

24 Admiral Rogers: Senator, I can't answer to the  
25 specifics of the National Guard Bureau. Let me only say

1 this. I am the son of a guardsman. My father was  
2 enlisted as an officer in the Illinois Guard for 25 years.  
3 This is the world I knew as a child, growing up. So, the  
4 Guard and the Reserve are something personally important  
5 to me. In fact, I just, coincidentally, sat down with a  
6 team over the last week and were just reviewing, What's  
7 the Guard and Reserve plan, the portion of the mission-  
8 force piece?

9 The point I think you make is both important. I'm the  
10 first to acknowledge that. And I will take an action from  
11 here to pull the string on this, because, I apologize, I  
12 just haven't seen that report, and I don't know the  
13 specifics. But, it is reflective. We have always  
14 maintained that, as we're building the breadth of  
15 capability for the Department in cyber, that the structure  
16 we have to come up with has to go way beyond just the  
17 Active piece, here, that the Guard and Reserve have got to  
18 a critical piece of what we do here, which is why, if you  
19 look at what the Air Force is doing, six of their 40 or so  
20 teams are Guard or Reserve. If you look at the Army, for  
21 example, they are bringing online an additional 22 Cyber  
22 Protection Teams from the Guard, purely associated with  
23 Guard and State missions, not necessarily the Cyber  
24 Mission Force, because they realize the importance of this  
25 investment. Marine Corps and Navy, there is -- their

1 approach, slightly different. Again, they don't have a  
2 Guard structure. Their approach, slightly different.

3 So, if I could, let me take for action that one and  
4 pull the strong. And then I apologize, I just don't --

5 Senator Ernst: No, I --

6 Admiral Rogers: -- have a good answer --

7 Senator Ernst: -- I certainly appreciate --

8 Admiral Rogers: -- for you there.

9 Senator Ernst: -- that. One team, one fight. I think  
10 there's a lot of capabilities that we are simply not  
11 utilizing or considering when we look at that big picture.  
12 So, I do appreciate that a lot.

13 [The information referred to follows:]

14 [COMMITTEE INSERT]

15

16

17

18

19

20

21

22

23

24

25

1        Senator Ernst: And are there steps that you think that  
2 you can take that would tie together better our Reserve  
3 component, our National Guard component? What kind of  
4 efforts can you assist with? What we can we assist with?

5        Admiral Rogers: So, I feel comfortable, overall, with  
6 the, quote, "Cyber Mission Force." Where I think the  
7 broader challenge for us is, What additional level of  
8 investment, as a Department and in a State structure, do  
9 we think that is appropriate, over and above that? And  
10 that's probably the biggest focus area for me, working  
11 with General Lengyel, about -- So, what should the future  
12 be? And then, whatever investments we make in the Guard  
13 and Reserve, how do we make sure that they are tied in and  
14 aligned with the broader Department effort? So, we're  
15 working this as one team. Because we just can't afford --  
16 everybody's out there doing their own thing. And that's  
17 just not going to get us where we need to be.

18        Senator Ernst: Right. Absolutely. I agree.

19        And then, gentlemen, for both of you, please. The  
20 Government Accountability Office also found that the  
21 yearly cyber exercise, Cyber Guard, failed to focus on  
22 emergency or disaster scenarios concurrent to cyber  
23 incidents, an area where the National Guard would be very  
24 helpful. And what efforts -- and again, you may not be  
25 tied as much into National Guard, but what efforts could

1 you take to improve Cyber Guard for the upcoming year --

2 Admiral Rogers: So --

3 Senator Ernst: -- so that we can focus on those --

4 Admiral Rogers: -- I haven't seen the specifics of the  
5 reports, but I will tell you that, not having read it,  
6 I'm, quite frankly, a little bit in disbelief, because I  
7 would tell you we call it Cyber Guard --

8 Senator Ernst: Right.

9 Admiral Rogers: -- for a reason, because it's focus  
10 on, How do we exercise, in an annual basis, the  
11 integration of the Guard, Reserve, and the Active  
12 component with industry? I spend time at that exercise  
13 every year. We just did it in June, down in Tidewater.  
14 Some members of the committee, in fact, actually came down  
15 and observed it.

16 So, I'm a little bit perplexed by the basic premise,  
17 but I haven't -- I apologize, I just haven't seen the  
18 specifics.

19 Senator Ernst: Okay. And I -- my time is running out.  
20 But, again, I think that demonstrates where we do need to  
21 put a little more emphasis on our Reserve-component forces  
22 and tie those in to our Active Duty component, as well,  
23 and really take advantage of the talent that exists out  
24 there, make sure that we're exercising their capabilities.

25 Admiral Rogers: Yes, ma'am.

1 Senator Ernst: So, thank you very much, gentlemen.

2 Thank you.

3 Senator Reed [presiding]: On behalf of Chairman  
4 McCain, let me recognize Senator McCaskill.

5 Senator McCaskill: Yes. I want to follow up with  
6 Senator Ernst's comments. I just came from a tour around  
7 Missouri, and I had the opportunity to see the cyber unit  
8 at Jefferson Barracks, the Guard cyber unit at Jefferson  
9 Barracks in St. Louis, and also the Cyber Warriors at the  
10 139th Airlift Wing at Rosecrans Air Force Base. Both were  
11 remarkable. Both surprised me. I was not aware -- and  
12 I'm not sure, candidly, you're aware -- of all these units  
13 and what their capabilities are, and what they're doing.  
14 And what Senator Ernst just said -- what was remarkable  
15 about the Guard unit in St. Louis was who these people  
16 were in their day jobs. We're talking about the very top  
17 level of cybersecurity at a Fortune 500 company that has  
18 huge needs in this area. Huge needs. I mean, this guy  
19 knows more, I would bet, than a huge number of the people  
20 that you are commanding within the Active military, in  
21 terms of both cyber offense and cyber defense.

22 And I've realized that this is a great opportunity for  
23 our Guard to recruit some of the most talented and  
24 technically capable people in the private sector, since  
25 the vast majority of the networks that we are supporting,

1 in terms of protection in this country, are, in fact,  
2 private networks.

3 And so, I wanted to bring that up with you and ask your  
4 opinion about that integration, and particularly as it  
5 relates to the lynchpin with the Department of Homeland  
6 Security. Because the beauty of the Guard is, it is busy  
7 with domestic security as part of their mission, because  
8 of the TAG and the involvement of State governments,  
9 whether it's a natural disaster or other kinds of  
10 problems. And so, it seems to me that utilizing the Guard  
11 as the lynchpin between the Department of Homeland  
12 Security and the Department of Defense would make a great  
13 deal of sense, Admiral Rogers. And I would like your  
14 comment on that.

15 Admiral Rogers: First of all, I agree with the  
16 fundamental premise that the Guard and the Reserve bring a  
17 lot of capability. That's one reason why the Cyber  
18 Mission Force idea is predicated as the idea -- it's our  
19 ability to bring it all together -- not just all Active,  
20 not just Guard; it's the ability to bring it together.

21 In terms of who should be the fundamental lynchpin --  
22 before I get into publicly endorsing a particular strategy  
23 or solution, this is just one I want to make sure we think  
24 our way through. Because in -- there are challenges if  
25 you do it Active-only. There's challenges if you do it

1 over Guard- or Reserve-only. And I'd also be interested:  
2 Hey, what's DHS's perspective in this?

3 One of the other challenges I've found so far in my  
4 time in command, we have to work our way through what --  
5 and this is where the Guard, I think, becomes incredibly  
6 critical -- what's the difference between -- we're using  
7 DOD capability to work Federal large critical  
8 infrastructure versus what is the capability DOD -- by  
9 extension, the Guard -- can bring to the fore at a much  
10 more localized State and local level? And that's an area  
11 that, clearly, the Guard is very optimized for, that the  
12 Active piece is not as readily optimized for.

13 Senator McCaskill: I'm sure one of our problems in  
14 this space is retaining Active personnel, because if they  
15 become very skilled in this area, the -- there's lots of  
16 lucrative opportunities in the private sector. Has there  
17 been any thought given to an active recruitment of these  
18 folks into the Guard as they move into the private sector  
19 for a lot more money and people not being able to tell  
20 them where they're going to live 24/7? Is it possible  
21 that we are losing an opportunity, in terms of retaining  
22 some of the talent that we have, by not directly  
23 recruiting them into the Guard?

24 Admiral Rogers: So, knock on wood, retention on the  
25 Active side is exceeding our expectations. That doesn't

1 mean it won't change tomorrow or next week or next month.

2 I will say, since the Guard is an Air Force and an  
3 Army-specific construct, I know both of those services, in  
4 my discussion with my subordinate commanders from them,  
5 talk about, how do we make sure, as we're watching the  
6 workforce transition out of the Active -- separate, retire  
7 -- is there a way to tie in the Guard piece? Senator Cruz  
8 mentioned San Antonio, for example. I've seen several  
9 instances in the San Antonio area, because they're such a  
10 large concentration, where this is working very well. I'm  
11 not sure how well it's working in those areas where we  
12 don't have this large Guard and Active --

13 Senator McCaskill: Right.

14 Admiral Rogers: -- complement of force, if it will.  
15 So, I just don't know, off the top of my head.

16 Senator McCaskill: And this idea has been discussed  
17 openly, and I know there is a lot of controversy around it  
18 and a lot of pros and cons, but one of these really  
19 talented cyber warriors at the Guard unit that I visited  
20 with, I was told that one of them almost was removed  
21 because of sit-ups. What about the PT requirement? And  
22 what value is there to forming an elite cyber squad that  
23 is civilian, as opposed to, you know, losing a really  
24 talented guy because of sit-ups?

25 Admiral Rogers: So, my first comment would be,

1 remember, the Law of Armed Conflict specifically  
2 prescribes what civilians and uniforms can do in some  
3 particular applications. So, I generally remind people, a  
4 lot of it would have to do with, what would the mission be  
5 that you gave that entity? Because there are some things  
6 in the Law of Armed Conflict that physically could not do.  
7 Uniforms have to do it, as opposed to --

8 Senator McCaskill: Right.

9 Admiral Rogers: -- application of force and  
10 capability.

11 To date, are there numbers where that is an issue?  
12 Clearly. I'm not going to pretend, for one minute. But,  
13 we have been able to retain people and still meet the  
14 requirements associated with the broader military without  
15 decreasing capability. If that changes over time, though  
16 -- it's one of the things I have talked about -- we need  
17 to be mindful that if circumstances change, we need to  
18 look about changing the rules that we currently operate.  
19 And if the situation were to change, those would be one of  
20 the things I would say, "So, do we need to look at a  
21 different force balance or mix? Do we" --

22 Senator McCaskill: Right.

23 Admiral Rogers: -- "need to look at a different set of  
24 standards or requirements associated with individuals?" I  
25 don't think we're at that point now, but if the situation

1 were to change, I think we would definitely need to do  
2 that.

3 Senator McCaskill: I would certainly urge that  
4 flexibility --

5 Admiral Rogers: Yes, ma'am.

6 Senator McCaskill: -- because I think this is going to  
7 be a growing part of our national security --

8 Admiral Rogers: Right.

9 Senator McCaskill: -- piece.

10 Admiral Rogers: Thank you.

11 Senator Reed: On behalf of the Chairman, let me  
12 recognize Senator King.

13 Senator King: Thank you, Mr. Chairman.

14 It seems to me the good news is that we're the most  
15 wired society on Earth. It gives us fantastic  
16 efficiencies and productivity and advantages, in many  
17 ways. But, the bad news is, we're the most wired society  
18 on Earth, which means we are the most vulnerable.

19 Admiral Rogers, you're familiar, I'm sure, with the  
20 Ukraine hack of the grid in December 2015. One of the  
21 things we learned from that is that there -- that hack was  
22 much less serious than it might have been, because of some  
23 retro technology --

24 Admiral Rogers: The antiquated --

25 Senator King: -- analog switches, old Demetri, who had

1 to go out and throw a switch somewhere at a relay. Do we  
2 have some lessons from that, that we ought to be thinking?  
3 And thinking about elections, it's hard to hack a paper  
4 ballot.

5 Admiral Rogers: Sir.

6 Senator King: Those kinds of things. Is that --  
7 should we be examining that area?

8 Admiral Rogers: I mean, we certainly are. I mean, one  
9 of the lessons, I think, from the Ukraine, for example,  
10 is, not only the analog, the physical piece, but also the  
11 way that their grid was broken down into components.

12 Senator King: Right.

13 Admiral Rogers: It's leading to some things. For  
14 example, as a naval officer, we're teaching celestial  
15 navigation again --

16 Senator King: I was going to bring that up.

17 Admiral Rogers: -- at the Naval Academy.

18 Senator King: I understand it's the first time in 20  
19 years that --

20 Admiral Rogers: Right, which we had stopped doing,  
21 because we said to ourselves, "Well, we have automated  
22 chart processes now. Why would we need to use celestial  
23 bodies to -- for navigation to define out" --

24 Senator King: Because you can't hack a sextant.

25 Admiral Rogers: Yes, sir. And so, we acknowledge that

1 there are things that we are going to need to look back,  
2 in this current world we're living in, and say to  
3 ourselves, "Perhaps some of the assumptions that we've  
4 made are not going to prove to be accurate." And we've  
5 got to ask ourselves, "What are the second- and third-  
6 order implications? What have we got to train  
7 differently? What skills do we need to have that we  
8 perhaps" --

9 Senator King: But, we also need to --

10 Admiral Rogers: -- "for the last 20 years have said we  
11 don't need?"

12 Senator King: As you -- as I think you've said, we  
13 need to question the basic assumption that digital is --

14 Admiral Rogers: Yes, sir.

15 Senator King: -- always better.

16 Admiral Rogers: Yes, sir.

17 Senator King: Senator Risch and I have a bill in  
18 before the Energy and Natural Resources Committee to ask  
19 the National Labs to work with the utilities to look at  
20 the Ukraine situation and see if there are places -- not  
21 to de-digitize the --

22 Admiral Rogers: Sir.

23 Senator King: -- grid, but places where there could be  
24 analog switches or other devices put in to deal with just  
25 --

1 Admiral Rogers: Right.

2 Senator King: -- just this issue.

3 Let me turn to encryption for a minute. While this  
4 hearing was going on -- and I don't want to sound like  
5 this was a big production -- in about, literally, a minute  
6 and a half, I downloaded Telegram. And Telegram is an  
7 app, as you know, that's encrypted. I thought it was  
8 interesting. I looked at what it -- how it works. It's  
9 fully encrypted. It's in English, Arabic, Dutch, German,  
10 Italian, Korean, Portuguese, and Spanish. It's -- was  
11 started by two brothers from Russia. It's based in  
12 Berlin. I mean, this is the reality, isn't it, Mr.  
13 Lettre, that we're -- we can't stop this. The idea of  
14 somehow being able to control encryption is just not  
15 realistic.

16 Mr. Lettre: We can't stop these trends, you're right,  
17 Senator. And individuals -- all of us benefit from strong  
18 encryption. The Department of Defense does. I personally  
19 am in favor of having strong encryption that allows me to  
20 protect my personal data. The challenge is -- and yet, we  
21 need to find our -- think our way through how we can  
22 continue to fulfill our responsibilities to enforce the  
23 laws and protect the Nation. And I think what we do find  
24 is, there are a number of instances where government  
25 leaders have been able to strike a very collaborative and

1 cooperative dialogue with key sectors in the text sector.  
2 Individual players and executives have been able to focus  
3 on finding --

4 Senator King: But, that --

5 Mr. Lettre: -- solutions.

6 Senator King: -- that worked pretty well in the '20s,  
7 when you were talking about the telephone system, which  
8 was only within the country. And you can -- we can deal  
9 with Apple or with Microsoft or with Cisco or whoever, but  
10 if you've got a cloud-based app that's -- the headquarters  
11 is in Berlin, and who knows where the data is -- I mean,  
12 we -- as hard it is for us to believe, there are places  
13 our power doesn't reach. We can't regulate something  
14 that's over in Berlin or Swaziland.

15 Mr. Lettre: That's a very good point. There will  
16 always be places across these sectors and these technology  
17 solutions that we just -- we may not be able to find a way  
18 forward. They may be -- the solution may be elusive.

19 Senator King: Well, I'd like --

20 Mr. Lettre: It does require us to think innovatively -

21 - Senator King: Well --

22 Mr. Lettre: -- even beyond encryption, about how we  
23 can continue to go after national security challenges.

24 Senator King: That was -- you know, the word  
25 "innovation" -- I mean, this is a -- this is the world

1 history of conflict, is invention, reinvention,  
2 reinvention, reinvention.

3 And I also want to associate myself with Senator Lee's  
4 questions. We also need to get back to old-fashioned  
5 human intelligence. And I think it's -- SIGINT was easy,  
6 in a sense, if you can pick up conversations. Now that  
7 that's no longer as easy as it once was, we need to be  
8 thinking about, what are the other techniques that we can  
9 use? They -- and it may be old-fashioned intelligence.  
10 It may also be other high-tech satellite or other things.  
11 But, it -- it's -- we can't -- I think innovation is going  
12 to be an absolute key to this.

13 Mr. Lettre: Yes. That's absolutely right, Senator.  
14 The -- in particular, as you pointed out, we do need to  
15 build innovation across a range of intelligence  
16 disciplines and collection capabilities. So, even in the  
17 human intelligence arena, we know how effective it can be.  
18 We also know that technology trends are changing how we do  
19 HUMINT. And we need to be able to adapt and invest in  
20 innovation, in how we conduct our human intelligence  
21 operations, as well.

22 Senator King: And my time is up, but I would suggest  
23 big data analysis is one of those tools.

24 Mr. Lettre: Absolutely.

25 Senator King: Thank you.

1 Thank you, Mr. Chairman.

2 Senator Reed: Thank you, Senator King.

3 On behalf of the Chairman, let me thank you gentlemen  
4 for your testimony today and your service.

5 And, since there are no other colleagues here, I would  
6 call the hearing adjourned.

7 Thank you.

8 [Whereupon, at 11:20 a.m., the hearing was adjourned.]

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