

Stenographic Transcript  
Before the

COMMITTEE ON  
ARMED SERVICES

**UNITED STATES SENATE**

HEARING TO RECEIVE TESTIMONY ON UNITED STATES  
CYBER COMMAND

Tuesday, May 9, 2017

Washington, D.C.

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

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

HEARING TO RECEIVE TESTIMONY ON  
UNITED STATES CYBER COMMAND

Tuesday, May 9, 2017

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

The committee met, pursuant to notice, at 9:35 a.m. in Room SD-G50, Dirksen Senate Office Building, Hon. John McCain, chairman of the committee, presiding.

Committee Members Present: Senators McCain [presiding], Inhofe, Wicker, Fischer, Cotton, Rounds, Ernst, Tillis, Sullivan, Perdue, Graham, Sasse, Strange, Reed, Nelson, McCaskill, Shaheen, Gillibrand, Blumenthal, Donnelly, Hirono, Kaine, King, Heinrich, Warren, and Peters.

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

3           Chairman McCain: Good morning.

4           The committee meets today for a hearing on the posture  
5 of the United States Cyber Command.

6           We are pleased to welcome back Admiral Mike Rogers, the  
7 Commander of U.S. Cyber Command, Director of the National  
8 Security Agency, Chief of the Central Security Service, and  
9 several other titles I believe. We are grateful for your  
10 many years of distinguished service and for your appearance  
11 before the committee today.

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

16          As a result, this committee has focused its attention  
17 on cybersecurity. We have expressed our concern at the lack  
18 of a strategy and policy for addressing our cyber threats.  
19 We were hopeful that after years without any serious effort  
20 to develop a cyber deterrence policy and strategy from the  
21 last administration, the new administration promised one  
22 within 90 days of the inauguration. But 90 days have come  
23 and gone and no such policy and strategy have been provided.

24          While inaction from the executive branch has been  
25 disheartening, this committee has not stood still. In fact,

1 this committee has adopted more than 50 provisions over the  
2 past 4 years focused on organizing, empowering, and enabling  
3 the Department of Defense to deter and defend against  
4 threats in cyberspace.

5 But cyber is an issue that requires an integrated,  
6 whole-of-government approach. We simply do not have that  
7 now. The very fact that each agency of government believes  
8 it is responsible for defending the homeland is emblematic  
9 of our dysfunction. We have developed seams that we know  
10 our adversaries will use against us. Yet, we have failed to  
11 summon the will to address these seams through reform.

12 Our allies, most notably, the United Kingdom, have  
13 recognized the need for a unified approach. I look forward  
14 to hearing from Admiral Rogers his assessment of the  
15 recently established National Cyber Security Centre in the  
16 UK and whether a unified model would help address some of  
17 our deficiencies here in the United States.

18 The Coast Guard also presents an interesting model that  
19 should be evaluated for addressing some of our cyber  
20 deficiencies. The Coast Guard has an interesting mix of  
21 authorities that may be just as applicable in cyberspace as  
22 they are in territorial waters. They are both an agency  
23 within the Department of Homeland Security, as well as a  
24 branch of the armed services. They can operate both within  
25 the United States and internationally and can seamlessly

1 transition from law enforcement to military authorities. A  
2 cyber analogue to the Coast Guard could be a powerful tool  
3 for addressing gaps that impede our existing organizational  
4 structure. It could also serve as a much-needed cyber first  
5 response team responsible for immediate triage and hand-offs  
6 to the appropriate federal entity for further response,  
7 remediation, or law enforcement action.

8 As for the efforts at the Department of Defense, I  
9 understand that Cyber Command is still on track to reaching  
10 full operational capability for the training of the Cyber  
11 Mission Force in the fall of 2018. But unless we see  
12 dramatic changes in future budgets, I am concerned these  
13 forces will lack the tools required to protect, deter, and  
14 respond to malicious cyber behavior. In short, unless the  
15 services begin to prioritize and deliver the cyber weapons  
16 systems necessary to fight in cyberspace, we are headed down  
17 the path to a hollow cyber force.

18 I also am concerned with the apparent lack of trained  
19 people ready to replace individuals at the conclusion of  
20 their first assignments on the Cyber Mission Force.  
21 Unfortunately, we have already heard about some puzzling  
22 issues. Specifically, out of the 127 Air Force cyber  
23 officers that completed their first tour on the Cyber  
24 Mission Force, none went back to a cyber-related job. That  
25 is unacceptable and suggests a troubling lack of focus. It

1 should be obvious the development of a steady pipeline of  
2 new talent and the retention of the ones we have trained  
3 already is essential to the success of the Cyber Mission  
4 Force.

5 Admiral Rogers, we look to you to help us better  
6 understand if we should take a closer look at if the  
7 existing man, train, and equip models of the services are  
8 sufficient or if we should consider a different model.  
9 Later this week, we plan to have another cyber hearing with  
10 outside experts of which we plan to ask if we should be  
11 considering the creation of a cyber service.

12 Admiral Rogers, welcome back. This is, I am sure, one  
13 of numerous pleasures you have of coming before this  
14 committee. Welcome.

15 Senator Reed?

16

17

18

19

20

21

22

23

24

25

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

3           Senator Reed: Well, thank you very much, Mr. Chairman.  
4 Let me join you in welcoming Admiral Rogers. And as you  
5 point out, Mr. Chairman, the frequency with which the  
6 Admiral is called up to testify to the committee is a  
7 testament of not just his importance, but the importance of  
8 cyber in the severe challenges we face in this domain. So,  
9 again, thank you Admiral, for your service and your  
10 dedication.

11           We have faced serious and growing threats in  
12 cyberspace, from espionage, theft of intellectual property,  
13 and destructive attacks on the networks and systems that  
14 support our military and our economy, including critical  
15 infrastructure. Now we and our allies in Europe are  
16 experiencing firsthand that we are also vulnerable to the  
17 manipulation and distortion of information through  
18 cyberspace, which Russia is exploiting to threaten the  
19 bedrock of our democracy and our shared international  
20 institutions.

21           The Armed Services Committee has for years emphasized  
22 the importance of developing the means and the strategy to  
23 deter cyber attacks. Now the scope of what we must defend  
24 against and deter has expanded, and the task takes on even  
25 greater urgency.

1           In just a year's time, we begin an election season once  
2 more, and the intelligence community has warned that  
3 Russia's election interference is likely to be a new normal.

4           While our decentralized election system has been  
5 designated as critical infrastructure, we lack an effective  
6 integrated and coordinated capability to detect and counter  
7 the kind of influence operation that Russia now routinely  
8 and continuously conducts. We do not yet have a strategy or  
9 capability to deter such actions through the demonstrated  
10 ability to conduct our own operations of this type.

11           Secretary Carter commissioned a Defense Science Board  
12 task force on cyber deterrence. Prominent former officials,  
13 such as former Under Secretary of Defense for Policy Dr.  
14 James Miller, served on this task force and have testified  
15 to this committee twice this year. They advocate rapidly  
16 developing the ability conduct operations for cyberspace to  
17 threaten, quote, what key leaders on the other side value  
18 the most, which in the case of Russia could included their  
19 own financial wellbeing and status in order to deter  
20 influence operations and cyber attacks against us.

21           Achieving a credible deterrent requires integration of  
22 capabilities and focused policy development across the  
23 Department of Defense, as well as through the whole of  
24 government involving DOD, the State Department, the  
25 intelligence community, DHS, and the Justice Department. We

1 have not seen evidence yet that the new administration  
2 appreciates these urgent problems and intends to address  
3 them.

4 For Cyber Command, specifically the committee has heard  
5 concerns that our military cyber forces are almost  
6 exclusively focused on the technical aspects of cyberspace  
7 operations, such as detecting network intrusions, expelling  
8 intruders, and figuring out how to penetrate the networks of  
9 adversaries. The concern is that this focus misses the  
10 crucial cognitive element of information operations  
11 conducted through cyberspace. Those actions are designed to  
12 manipulate perceptions and influence decision-making.

13 Admiral Rogers, these are critical issues, and there is  
14 much work to do. And I look forward to your testimony and  
15 your views on these urgent matters. Thank you, sir.

16 Thank you, Mr. Chairman.

17 Chairman McCain: Welcome back, Admiral.

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: Thank you, sir.

5           Chairman McCain, Ranking Member Reed, and members of  
6           the committee, thank you for your enduring support and the  
7           opportunity today to talk about the hardworking men and  
8           women of United States Cyber Command. I welcome the  
9           opportunity to describe how Cyber Command conducts efforts  
10          in the cyberspace domain and supports the Nation's defense  
11          against sophisticated and powerful adversaries.

12          The Department of Defense recognized 7 years ago that  
13          the Nation needed a military command focused on cyberspace.  
14          U.S. Cyber Command and its subordinate elements have been  
15          given the responsibility to direct, operate, secure, and  
16          defend the Department's systems and networks which are  
17          fundamental to the execution of all DOD missions.

18          The Department and the Nation also rely on Cyber  
19          Command to build ready cyber forces and to be prepared to  
20          employ them when significant cyber attacks against the  
21          Nation's critical infrastructure require DOD support.

22          The pace of international conflict and cyberspace  
23          threats has intensified over the last few years. Hardly a  
24          day has gone by during my tenure at Cyber Command that we  
25          have not seen at least one significant cybersecurity event

1 occurring somewhere in the world. This has consequences for  
2 our military and our Nation at large. We face a growing  
3 variety of advanced threats from actors who are operating  
4 with evermore sophistication, speed, and precision. At U.S.  
5 Cyber Command, we track state and non-state adversaries as  
6 they continue to expand their capabilities to advance their  
7 interests in and through cyberspace and try to undermine the  
8 United States national interests and those of our allies.

9 Conflict in the cyber domain is not simply a  
10 continuation of kinetic operations by digital means. It is  
11 unfolding according to its own logic, which we are  
12 continuing to better understand. And we are using this  
13 understanding to enhance the Department and the Nation's  
14 situational awareness and management of risk.

15 I want to update you on our initiatives and plans to  
16 address that issue of situational awareness and risk  
17 management.

18 Our three lines of operations are to provide mission  
19 assurance for DOD operations and defend the Department of  
20 Defense information environment; to support joint force  
21 commander objectives globally; and to deter and defeat  
22 strategic threats to U.S. interests and critical  
23 infrastructure.

24 We conduct full spectrum military cyberspace operations  
25 to enable actions in all domains, ensure the U.S. and allied

1 freedom of action in cyberspace, and deny the same to any  
2 adversaries.

3 Defense of DOD information networks remains our top  
4 priority, of course, and that includes weapon systems,  
5 platforms and data. We are completing the build-out of the  
6 Cyber Mission Force, as you heard the chairman indicate,  
7 with all teams scheduled to be fully operational by the end  
8 of fiscal year 2018. And with the help from the services,  
9 we are continually increasing the Cyber Mission Force's  
10 readiness to hold targets at risk.

11 Your strong and continuing support is critical to the  
12 success of the Department in defending our national security  
13 interest, especially as we comply with the recent National  
14 Defense Authorization Act directive to elevate Cyber Command  
15 to unified combatant command status. As you well know, I  
16 serve as both Commander of U.S. Cyber Command and Director  
17 of the National Security Agency. This dual-hat appointment  
18 underpins the close partnership between Cyber Command and  
19 NSA, a significant benefit in cyberspace operations. The  
20 institutional arrangement for providing that support,  
21 however, may evolve as Cyber Command grows to full  
22 proficiency in the future. The National Defense  
23 Authorization Act in a separate provision also described  
24 conditions for splitting the dual-hat arrangement once that  
25 can happen without impairing either organization's

1 effectiveness,. This is another provision I have publicly  
2 stated that I support pending the attainment of certain  
3 critical conditions.

4 Cyber Command will also engage with this committee on  
5 several other matters relating to the enhancement of the  
6 command's responsibilities and authorities over the coming  
7 year. This would include increasing our cyber manpower,  
8 increasing the professionalization of the cyber workforce,  
9 building capacity, and developing and streamlining  
10 acquisition processes. These are critical enablers for  
11 cyberspace operations in a dynamically changing global  
12 environment.

13 Most or all of these particulars have been directed in  
14 recent National Defense Authorization Acts, and along with  
15 the Office of the Secretary of Defense for Policy and the  
16 Joint Staff, we will work with you and your staffs to iron  
17 out the implementation details.

18 Cyber Command personnel are proud of the roles they  
19 play in our Nation's cyber efforts and are motivated to  
20 accomplish their assigned missions overseen by the Congress  
21 and particularly this committee. They work to secure and  
22 defend DOD's systems and networks, counter adversaries, and  
23 support national and joint warfighter objectives in and  
24 through cyberspace. The command's operational successes  
25 have validated concepts for creating cyber effects on the

1 battlefield and beyond. Innovations are constantly emerging  
2 out of operational necessity, and the real world experiences  
3 we are having in meeting the requirements of national  
4 decision-makers and joint force commanders continue to  
5 mature our operational approaches and effectiveness over  
6 time.

7 This, combined with agile policies, faster decision-  
8 making processes, increased capabilities, broader concepts  
9 of operations and smarter command and control structures,  
10 will ensure that Cyber Command attains its full potential to  
11 counter adversary cyber strategies.

12 The men and women of Cyber Command thank you for your  
13 support and appreciate your continued support as we confront  
14 and overcome the challenges that lie ahead of us. We  
15 understand that a frank and comprehensive engagement with  
16 Congress not only facilitates the support that allows us to  
17 accomplish our mission, but it also ensures that our fellow  
18 citizens understand and endorse our efforts executed on  
19 their behalf. I have seen the growth in the command's size,  
20 budget, and mission. That investment of resources, time,  
21 and effort is paying off, and more importantly, it is  
22 helping to keep Americans safer not only in cyberspace but  
23 in other domains as well.

24 I look forward to continuing the dialogue of the  
25 command and its progress with you in this hearing today and

1 in the months to come. I look forward to answering your  
2 questions.

3 [The prepared statement of Admiral Rogers follows:]

4  
5  
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, Admiral.

2 We have seen another Russian attempt to affect the  
3 outcome of the election in France. Do you see any  
4 slackening, a reduction in Russian/Chinese efforts to commit  
5 cyber attacks and even affect elections?

6 Admiral Rogers: No, I do not.

7 Chairman McCain: Have you seen any reduction in  
8 Russian behavior?

9 Admiral Rogers: No, I have not.

10 Chairman McCain: The Defense Science Board told this  
11 committee, at least for the next decade, the offensive cyber  
12 capabilities of our most capable adversaries are likely to  
13 far exceed the United States' ability to defend key critical  
14 infrastructures. Do you agree with that assessment of the  
15 Defense Science Board?

16 Admiral Rogers: I agree that the offensive side in  
17 general has the advantage over the defense, which is why the  
18 ideas of deterrence are so important here. How do we shape  
19 and change opponents' behavior?

20 Chairman McCain: In order to do that, we would have to  
21 have a policy followed by a strategy. Right?

22 Admiral Rogers: Yes, sir.

23 Chairman McCain: Do we have that now?

24 Admiral Rogers: No, sir, but the new team is working  
25 on that. I want to make sure we all understand that.

1 Chairman McCain: And the check is in the mail?

2 So do you agree we should -- we have got the Federal  
3 Bureau Investigation as the lead for law enforcement. The  
4 Department of Homeland Security is the lead for critical  
5 infrastructure and defending government computer networks.  
6 And the Department of Defense is the lead for defending the  
7 homeland, defending military computer networks, and  
8 developing and employing -- is the status quo sustainable?

9 Admiral Rogers: It is sustainable, but my question is,  
10 is it the most effective way to generate outcomes.

11 Chairman McCain: Is it the most effective? That is a  
12 better question. Thank you.

13 Admiral Rogers: Yes, sir. My recommendation, my input  
14 to this process has met our challenges. So we built a  
15 foundation with a series of very specialized and distinct  
16 responsibilities, and yet I think what experience has taught  
17 us over the last few years is our ability to respond in a  
18 much more integrated, focused way is really the key to  
19 success here. And I think that is the challenge. How do we  
20 more formally integrate these capabilities across the  
21 government?

22 Chairman McCain: Do we need a cyber corps?

23 Admiral Rogers: I am not a proponent. Within the DOD,  
24 I am not a proponent of the idea of a separate cyber force  
25 or service, and that is for the following reasons. In my

1 experience, to be successful in cyber, you not only need to  
2 understand the technical aspects of this, but you need to  
3 understand the broader context in which cyber evolutions  
4 occur. Somewhere in the world, there is a man or woman  
5 sitting on a keyboard directing an operation. And so my  
6 concern is if we went with a very unique service approach to  
7 this, we would generate a force that was incredibly  
8 technically proficient but not necessarily deep in  
9 understand of the broader context. And I think using a  
10 service-based model is a stronger way to go about doing  
11 this.

12 Chairman McCain: Well, as I mentioned in my opening  
13 remarks, 127, whatever it is, in the Air Force. Not a  
14 single one stayed in cyber. Are you getting the kind of  
15 cooperation that you need to have trained people at work in  
16 your command?

17 Admiral Rogers: So I have talked to all the service  
18 chiefs personally over the course of the last year on this  
19 topic. I have one service that I am particularly  
20 highlighting to them saying, look, we need to change the  
21 policies here. What I have suggested to the services is the  
22 Cyber Mission Force, that part which I am responsible for, I  
23 acknowledge is only one part of the Department's broader  
24 cyber needs.

25 Chairman McCain: Was that message received by the

1 United States Air Force?

2 Admiral Rogers: They are clearly still working their  
3 way through this. They have a broader set of challenges  
4 with respect to manpower at large. I personally had a chief  
5 of staff of the Air Force come out to Fort Meade. I sat him  
6 down and said here is what I am seeing. Do I have the right  
7 picture? Is this accurate? He has come back to me and  
8 said, no, Mike, you have an accurate sense that we are not  
9 where we need to be, and here is what I am trying to do to  
10 get there. And so my job is to help him and also to keep  
11 the pressure on to make sure we sustain this.

12 Chairman McCain: In your job, you have to look at  
13 scenarios. Give us the best scenario and the worst  
14 scenario.

15 Admiral Rogers: For?

16 Chairman McCain: For cyber attacks on the United  
17 States.

18 Admiral Rogers: The worst worst case scenario in my  
19 mind has a couple dimensions to it: outright destructive  
20 activity focused on some aspects of critical  
21 infrastructure --

22 Chairman McCain: Including space?

23 Admiral Rogers: It could be space. And then in  
24 addition to outright destruction, the other thing that  
25 concerns me -- there are two other things. The second thing

1 would be, in terms of worst consequence, do we see data  
2 manipulation on a massive scale. Most cyber activity data  
3 has been penetration and extraction.

4 Chairman McCain: Like changing voting rolls.

5 Admiral Rogers: Yes. So what happens if we go in and  
6 we change data? That is a very different kind of challenge  
7 for us.

8 And then thirdly to me the other element of a worst  
9 case scenario, what happens when non-state actors decide  
10 that cyber now is an attractive weapon that enables them to  
11 destroy the status quo. That is kind of the worst end, if  
12 you will.

13 Chairman McCain: And the best.

14 Admiral Rogers: The best is --

15 Chairman McCain: We develop a policy followed by a  
16 strategy --

17 Admiral Rogers: We continue to make improvements both  
18 in capacity, as well as the broader deterrence piece.

19 Chairman McCain: Thank you, Admiral.

20 Senator Reed?

21 Senator Reed: Well, thank you, Mr. Chairman.

22 Again, thank you, Admiral.

23 As you have pointed out and I think we both pointed  
24 out, in terms of technical aspects of cyber, detecting  
25 intrusions, preventing intrusions, penetrating other

1 networks, Cyber Command has been in the forefront. But this  
2 issue, which you allude to, of cognitive operations,  
3 information warfare, changing public opinion, et cetera --  
4 have you been tasked to conduct such operations -- to  
5 prepare to conduct such operations?

6 Admiral Rogers: No, we have not. That is not right  
7 now in our defined set of responsibilities per se.

8 Senator Reed: Is it in anybody's federal  
9 responsibility to your knowledge?

10 Admiral Rogers: I will not get into the specifics in  
11 an unclassified forum. There are some things we are doing  
12 right now, for example, in the fight against ISIS with  
13 combatant commanders in this regard. And I do not want to  
14 go any deeper, if I could.

15 Senator Reed: That is fine.

16 Admiral Rogers: But I think one of our challenges is  
17 if information is now truly going to become a weapon almost  
18 in many ways, how are we going to optimize ourselves to deal  
19 with this world? And we had much of this skill. If you go  
20 back to the Cold War, when I first started my journey in  
21 uniform, we had extensive infrastructure, extensive  
22 expertise. As the Soviet Union collapsed, we decided  
23 perhaps that expertise is not required. We did away with  
24 many of the institutions. Many of the individuals who had  
25 the skill sets are no longer with us. I think we need to

1 step back and reassess that.

2 Senator Reed: So I would assume if you have not been  
3 tasked to do that, that your expertise in cognitive warfare  
4 is rather limited in terms of what you just mentioned, the  
5 skill sets, the personnel.

6 Admiral Rogers: Yes, sir. I would be the first to  
7 admit it is not what our workforce is optimized for.

8 Senator Reed: And certainly not comparable to what we  
9 are perceiving from other actors around the globe.

10 Admiral Rogers: Certainly not on a day-to-day basis.

11 Senator Reed: Within DOD, my knowledge suggests that  
12 SOCOM has been given the lead on information operations.

13 Admiral Rogers: Broadly.

14 Senator Reed: Broadly. And is there any integration  
15 with Cyber Command?

16 Admiral Rogers: Oh, we work very -- SOCOM is one of  
17 those partners that I mentioned. So we do work very  
18 closely, General Thomas and I.

19 Senator Reed: I think the other issue too -- and it  
20 has come up in the context of all of our comments this  
21 morning -- is that this is a mission that goes across  
22 several different organizations. And in fact, we have heard  
23 comments about how the State Department in some areas has --  
24 go back to the Cold War. They were doing the Voice of  
25 America. They were doing all the radio towers. It is a new

1 world. And they do not have either the expertise or the  
2 resources, et cetera. So no one seems to be doing this  
3 aggressively. Is that a fair estimate?

4 Admiral Rogers: Certainly we are not where we need to  
5 be.

6 Senator Reed: In terms of Russian operations, were you  
7 aware of the penetration of the election in 2016 in terms of  
8 the active involvement of Russian entities directly or  
9 indirectly?

10 Admiral Rogers: Yes, sir.

11 Senator Reed: What actions did you take? Just simply  
12 informing your superiors? Was that it?

13 Admiral Rogers: So here is where I have to  
14 differentiate between my role as Commander of Cyber Command  
15 and the Director of the National Security Agency. As the  
16 Director of the National Security Agency, as I have publicly  
17 testified before other committees, when NSA first gained  
18 initial knowledge in the summer of 2015 that the Russians  
19 were engaged in an effort to access political institutions,  
20 we informed the Federal Bureau of Investigation, which has  
21 overall responsibility to inform those organizations. As  
22 the Director of NSA, I do not deal directly with them.

23 In turn, I then make sure that DOD and other elements  
24 within the government have that awareness. That is where my  
25 role as Cyber Command comes in. So at Cyber Command, I

1 become aware of efforts in terms of intrusions and hacks  
2 directed against U.S. infrastructure. I turn to myself and  
3 make sure that the DOD system is optimized to withstand --  
4 because they were coming after DOD at the same time. In  
5 addition, we coordinate with the Department of Homeland  
6 Security. Is there a requirement? Are you looking for DOD?  
7 For example, if we had defined the voting infrastructure as  
8 critical infrastructure, then under the set of duties  
9 assigned to Cyber Command, had the President or the  
10 Secretary of Defense determined that DOD needed to insert  
11 themselves in this, I would have been tasked to do that at  
12 Cyber Command.

13 Senator Reed: And so if you had been tasked, you would  
14 have been prepared technically to try to disrupt these  
15 operations.

16 Admiral Rogers: Yes.

17 Senator Reed: And then again, given -- I am sure we  
18 have all been looking back. And the after-action reports  
19 are still being written about 2016. In your estimate, we  
20 have to be much, much better prepared for 2018 and beyond.  
21 Is that fair?

22 Admiral Rogers: I apologize, Senator.

23 Senator Reed: After looking at the experience in 2016,  
24 as you just described, knowledge of penetration, attribution  
25 to a foreign state, going after key systems in this country,

1 some of which have now been designated as critical  
2 infrastructure, we have to be much, much better prepared for  
3 2018, 2020, and beyond.

4 Admiral Rogers: I agree. I apologize. I did not hear  
5 that.

6 Senator Reed: No, no. That is fine, sir. Thank you  
7 very much.

8 Chairman McCain: Senator Inhofe?

9 Senator Inhofe: Admiral Rogers, it would be unfair for  
10 me to ask you to evaluate the article I showed you this  
11 morning because you have not read it yet. The title pretty  
12 much says it. It says -- it appeared this morning -- are  
13 cyber crooks funding North Korea's nukes? How does Kim  
14 Jung-un come up the billions to pay for nuclear tests.  
15 Increasingly successful online bank heists provide a lot of  
16 the funding. Does that make sense to you?

17 Admiral Rogers: So I am not going to get into  
18 specifics in an unclassified forum, but we have publicly  
19 acknowledged we have seen the North Koreans use cyber in a  
20 criminal mechanism, if you will, to generate monetary  
21 resources.

22 Senator Inhofe: It has to come from somewhere.

23 Admiral Rogers: Yes, sir.

24 Senator Inhofe: And when you look at it, you kind of  
25 eliminate -- you come down to that conclusion that they

1 might be right on this.

2 Admiral Rogers: Although I would highlight this is  
3 only one element of the North Korean broader attempts to  
4 generate revenue and get it back to North Korea.

5 Senator Inhofe: Well, you know, when we look and see  
6 the growth in this thing from 2006 to 2015, the number of  
7 cyber attacks has climbed by 1300 percent. And we have all  
8 visited about the policy or the lack of policy in making the  
9 decision. There is some thought that maybe there is too  
10 much authority at the top. It was General Goldfein that was  
11 quoted in December of last year. Actually before this  
12 committee, he said if we want to be more agile, then the  
13 reality is that we are going to have to push decision  
14 authority down to some lower levels in certain areas. Does  
15 that make sense?

16 Admiral Rogers: Yes, sir. And we have highlighted in  
17 the cyber arena to Secretary Mattis, as he has assumed his  
18 new responsibilities, I think this is an important area that  
19 we need to reassess particularly within the cyber arena.

20 Senator Inhofe: Just a matter of a few weeks ago, we  
21 happened to be in Israel and we met and talked to their  
22 national cyber director, Dr. Eviatar Matania, for a cyber  
23 subcommittee meeting. He actually came over and we had --  
24 it was Senator Rounds who was with me at that time. And of  
25 course, he chairs the subcommittee. And we had a meeting

1 that I think was pretty productive. Dr. Matania was pretty  
2 careful not to say that perhaps they might be doing  
3 something better there than we are doing. He said it is  
4 much more complex in the United States because of the size  
5 and all of that. But he also pointed out three things that  
6 were significant. And I just wonder if you had any thoughts  
7 or if you studied their system and maybe some other  
8 countries too to see what they are doing.

9 Admiral Rogers: With the case of Dr. Matania, there is  
10 a reason why every time I am in Tel Aviv, I see him, and  
11 every time he is in the United States, he sees us.

12 Senator Inhofe: I knew that was the case. He said the  
13 same thing.

14 Admiral Rogers: So we can learn from each other. In  
15 fact, we are talking about some potential test cases that we  
16 could use with a new team in place. So we will see how that  
17 plays out over time. But I look to him.

18 One of the things that I have learned in my journey in  
19 cyber is there is no one single organization, group, or  
20 entity that has all the answers. So it is about the power  
21 of partnerships here and how do you create a system that  
22 enables you to gain insight and knowledge from a whole host  
23 of partners, some within the United States, outside the  
24 United States, within the government, the academic world,  
25 industry. He is one example of the power of that.

1 Senator Inhofe: I kind of got that impression too.

2 When General Alexander was in that position, he spent  
3 some time out at the University of Tulsa. And I know there  
4 are many other schools too. The chairman asked the  
5 question, are we having access to the people that are going  
6 to become necessary to staff this new, very serious problem  
7 that we have? Is there an effort going back to some of  
8 these schools and to promote the programs as were promoted  
9 in that particular university?

10 Admiral Rogers: Oh, there is. Between NSA and Cyber  
11 Command, we have relationships right now with over 200  
12 academic institutions around the United States because that  
13 is in part the future workforce for us, although one thing I  
14 try to highlight is be leery of creating a cyber force where  
15 everyone is cookie cutters. We need to get a broad range of  
16 skills and experience here. And some people are going to be  
17 really good at this, and they will not necessarily have  
18 advanced education, but they have spent much of their  
19 personal life in this. So we have got to build a construct  
20 where we can get that full spectrum of capability.

21 Senator Inhofe: We look and we see what some of these  
22 countries are doing. Putin, when he came in after their  
23 parliamentary election and they did not have any communists  
24 for the first time in 96 years -- he started doing things in  
25 addition to just the coming in and declaring a level of

1 warfare. He also started working. And apparently,  
2 according to Poroshenko, they have used cyber capabilities  
3 to attack the Ukrainian Government more than 6,500 times  
4 over the last 2 months. So this is something that is  
5 happening. It is happening all over the world. And you see  
6 something like the example in Ukraine that did not take any  
7 lead time, and all of a sudden, they are already inflicting  
8 that type of harm. And I am sure that you are right on top  
9 of everything that is happening with this.

10 Admiral Rogers: We are trying.

11 Senator Inhofe: Thank you very much.

12 Chairman McCain: Senator Nelson?

13 Senator Nelson: Thank you, Mr. Chairman.

14 And thank you, Admiral, for your public service.

15 In response to Senator Reed, you said that you were  
16 aware of Russian attempts to interfere in our election.  
17 Were you aware of Russian communications with members of the  
18 Trump campaign team?

19 Admiral Rogers: Now you are into my role as NSA. I am  
20 here as Cyber Command. I am not going to publicly get into  
21 that, sir.

22 Senator Nelson: I understand your reluctance, but I  
23 also see you not just Cyber Command. I see you as the NSA  
24 Director. Okay.

25 The chairman mentioned and asked you is this what we

1 see -- this behavior -- is this a new normal, to which you  
2 responded I think somewhat regretfully yes.

3 Admiral Rogers: Yes, sir.

4 Senator Nelson: How should we counter these kind of  
5 cyber-enabled information operations, and who has the  
6 responsibility for these kind of operations?

7 Admiral Rogers: In terms of Russian execution of the  
8 operations or our response? I apologize. I am trying to  
9 understand.

10 Senator Nelson: Both.

11 Admiral Rogers: Both. Well, in the case of the  
12 Russians, again if you refer to the publicly available  
13 intelligence community assessment, we identified multiple  
14 Russian security elements that were involved in this  
15 campaign.

16 With respect to what should we do, the first is I think  
17 we need to publicly out this behavior. We need to have a  
18 public discourse on this. Those nation states, groups, or  
19 individuals that would engage in this behavior -- they need  
20 to know that we are willing to publicly identify them and  
21 publicly identify the behavior.

22 Secondly, I think we have got to make this much more  
23 difficult for them to succeed. That means hardening our  
24 systems, taking a look at our election process, which is not  
25 Cyber Command's role, but I think broadly we need to look at

1 this end to end and ask ourselves what changes do we need to  
2 make in this structure.

3 Thirdly, I think as a society, as a Nation, we need to  
4 acclimatize ourselves to the idea that we are, in many ways,  
5 back into a time frame of disinformation, false news -- it  
6 goes to Senator Reed's point -- manipulation of media. You  
7 got to be a much more discerning reader, so to speak, in  
8 many ways in the world that we are living in right now.

9 And then lastly, I think we also need to make it very  
10 clear to those nation states or groups that would engage in  
11 this behavior it is unacceptable, and there is a price to  
12 pay for doing this.

13 Senator Nelson: So at this point, it sounds, listening  
14 to the answers to the previous questions, that we are really  
15 in a position that we cannot prevent a cyber attack on  
16 things like our critical infrastructure.

17 Admiral Rogers: Again, when we say prevent, it is one  
18 of the reasons why deterrence becomes so important. The  
19 goal should be we want to convince actors you do not want to  
20 do this. Regardless of whether you could be successful or  
21 not, it is not in your best interest, and you do not want to  
22 engage in this behavior.

23 Senator Nelson: In a different setting that is secure,  
24 would you share with us where we have either, under the  
25 threat of an attack or an attack, deterred, the word you

1 just used -- "deterrence" -

2 Admiral Rogers: Yes, sir. I can share with you in a  
3 classified setting where we have either driven them out of a  
4 network or --

5 Senator Nelson: That would be very helpful.

6 Now, would you consider a critical infrastructure voter  
7 registration rolls?

8 Admiral Rogers: I think that one of the challenges --  
9 if you go back to the process we used to identify the  
10 current 16 defined critical infrastructure areas in the  
11 private sector, we tended to look at that from a very  
12 industrial -- is there an output associated with it? One of  
13 the things I think that we need to be thinking about now is  
14 not that an output is not important because an election  
15 generates an output, but does data and information exist in  
16 areas that is of critical consequence to us as a Nation. We  
17 really did not look at it that way in simplistic terms, and  
18 I think we need to. We need to reassess it.

19 Senator Nelson: We sure better because if someone  
20 shows up to vote and suddenly they find out they are not a  
21 registered voter because, indeed, it has been attacked and  
22 the data has been manipulated and taken them off the rolls,  
23 that is pretty serious.

24 Admiral Rogers: Yes, sir.

25 Senator Nelson: And that is critical infrastructure.

1           Admiral Rogers: Yes, sir. We need to take a look at  
2 that definition.

3           Senator Nelson: Thank you, Mr. Chairman.

4           Chairman McCain: Senator Wicker?

5           Senator Wicker: Thank you.

6           Let me follow up on the chairman's statement with  
7 regard to the Air Force cyber officers not remaining in that  
8 field of work. Would one of the reasons be because they do  
9 not view it as a good career path?

10          Admiral Rogers: No. If I could say when we say not in  
11 that field, the experience we are seeing is they are taking  
12 officers that are rolling out of the Cyber Mission Force,  
13 that structure that I am responsible for, and employing them  
14 in other areas in cyber in the Department. That is why I  
15 say part of the challenge, if you are a service, you have a  
16 wide spectrum of cyber requirements beyond just what Cyber  
17 Command is responsible for. It is why I am trying to make  
18 the argument with the services what we need to do is -- and  
19 I have talked to them and said, look, I think something on  
20 the order of a third should stay with us, the rest we should  
21 then look how do we put them elsewhere with this within this  
22 broader cyber enterprise to build the cyber level of  
23 expertise across the Department.

24          I do not want to make it sound like what the Air Force  
25 is doing is just ripping people, once they finish their 3

1 years with us, so to speak, and then making them airplane  
2 mechanics, for example. That is not what we are seeing at  
3 all.

4 Senator Wicker: Okay. For the third you would like to  
5 keep, do you think that is a good way to get to be a four-  
6 star?

7 Admiral Rogers: Oh. Do you mean could you build a  
8 career over time?

9 Senator Wicker: Right.

10 Admiral Rogers: Clearly in the military we are moving  
11 into, I am not the last person who is going to be doing this  
12 as a four-star I do not think.

13 Senator Wicker: And then with regard to the cyber  
14 service, which you are doubtful about, do I understand  
15 Britain does have such a cyber force?

16 Admiral Rogers: No. Their structure is less a cyber  
17 service and more a combination of active as well as  
18 significant reserves.

19 Senator Wicker: Is anybody trying this? Are any of  
20 our allies trying this?

21 Admiral Rogers: There is nobody right now who has  
22 really gone to a single cyber service. Most are trying to  
23 take -- within the existing service structure, can you  
24 create a dedicated work specialty, so to speak, where that  
25 is what you do for your career. That is what is being done

1 by most nations around the world.

2 Senator Wicker: Well, keep us posted on that.

3 Now, on page 2 of your written testimony, you say  
4 advanced states continue to maintain the initiative just  
5 short of war, challenging our ability to react and respond.  
6 Unquote.

7 So what constitutes an act of war in your opinion or in  
8 terms of the policy of the agency?

9 Admiral Rogers: So, first, I am not a lawyer and I am  
10 not a policy individual. And that question at its heart is  
11 about legality and policy.

12 It is clear that we do not -- and not just the United  
13 States. I would argue broadly internationally we have not  
14 yet reached a broad consensus on how you would define in  
15 clear, actionable terms what an act of war within the cyber  
16 arena looks like. And to date --

17 Senator Wicker: How are we going to do that?

18 Admiral Rogers: We are going to get our policy people  
19 together. And we are trying to discuss this broadly.  
20 Again, it is outside my lane, but I know we are involved in  
21 broad discussions both internally within the U.S.  
22 Government, as well as with foreign partners, about how we  
23 develop a broader consensus on that.

24 Senator Wicker: Well, help us out, though, because it  
25 may not be in your lane. You are not a lawyer you say. But

1 you would certainly be one of the first people I would ask  
2 in terms of what sort of act in your judgment would go  
3 beyond this threshold of war.

4 Admiral Rogers: Personally for me, what I look to do  
5 is could we define a set of criteria, intent, impact, the  
6 tactics or techniques that were used, for example -- could  
7 we develop a set of very specific criteria that would help  
8 us define this rather than this broad -- "nebulous" is the  
9 wrong word because it implies people are not really focused  
10 on it, but this rather general kind of conversation we often  
11 tend to find ourselves in. I am trying to mentally work  
12 myself through how could we get this down to a more specific  
13 set of attributes that would then help us. I see those  
14 attributes that, therefore, would be defined as an act of  
15 war as an example.

16 Senator Wicker: And one other thing. You say  
17 technical developments are outpacing laws and policies. We  
18 certainly find that in the commerce area also.

19 But do you need anything new in this next NDAA that you  
20 do not have now?

21 Admiral Rogers: Specific to the NDAA in broad terms,  
22 my input to the process has been we need to reassess  
23 authorities and delegation. We need to take a look at do we  
24 have the right investments in manpower. Are we investing in  
25 the right capabilities? I am very honored that the

1 Department has focused on this mission. There should not be  
2 any doubt in anybody's mind. There is focus on this mission  
3 set. And I am the first to acknowledge cyber competes with  
4 a broader range of priorities and needs. But the argument I  
5 am trying to make is within those priorities, I think cyber  
6 is pretty high and we need to focus the investment and  
7 prioritize it and we cannot be willing to accept 5 to 10  
8 years for development cycles, whether it is getting the  
9 right people, whether it is training them. That is just not  
10 going to get us where we need to be.

11 Senator Wicker: To the extent that laws and policies  
12 are being outpaced, tell us what you need. Let us know what  
13 you need.

14 Admiral Rogers: Yes, sir.

15 Chairman McCain: Senator Gillibrand?

16 Senator Gillibrand: Thank you, Mr. Chairman.

17 Following the line of questioning by Senators Nelson  
18 and Reed, one of the issues raised by Russian intervention  
19 in our election is how our government as a whole responds to  
20 cyber attacks and how it escalates its response. Do you  
21 believe that there is a coherent plan in place to allow the  
22 Federal Government, in coordination with State and local  
23 governments, to respond to major cyber attacks on the  
24 country and to escalate the response as appropriate?

25 Admiral Rogers: To be honest, Senator, I do not know

1 enough to accurately answer the question because some parts  
2 of that strategy would be outside my purview, and I am just  
3 not smart about all the -- I am not trying to be a smart  
4 ass, but part of this is just outside my knowledge. So I am  
5 just not in a position to say categorically yes or no.

6 Senator Gillibrand: So I was concerned by your earlier  
7 responses that your strategy is deterrence because I do not  
8 see how deterrence is going to work with regard to Russia  
9 since we have seen a continuation of an interest on their  
10 part to hack our systems and hack other countries' systems  
11 and their elections. So I guess what I am looking for from  
12 you is leadership in coordination with other government  
13 agencies throughout the U.S. Government to be prepared for  
14 our next election.

15 Admiral Rogers: Oh, yes, ma'am. I am part of this.

16 If I could, I do not think you heard me say that I  
17 thought our strategy was deterrence. What I thought at  
18 least I communicated was deterrence should be a part of a  
19 broader strategy. It should not be the only thing. I am  
20 the first to acknowledge that.

21 Senator Gillibrand: Do you think particularly the  
22 transition between private companies and a government  
23 response -- are there the authorities in place to accomplish  
24 these transitions effectively? And if not, what kind of  
25 authorities might you need?

1           Admiral Rogers: I do not know if it is -- there is  
2 certainly an authorities aspect to it, but part of this, I  
3 am wondering, is cultural. So the government comes to a  
4 private entity. And you saw this in the Russian hack  
5 scenario. And the government informs this private entity  
6 the Russians have penetrated your system. Here is where  
7 they are. In some cases, the responses are, hey, we want to  
8 work with you. That is great. Thanks. Can we come back?  
9 In some cases, it is thanks very much, and we never hear  
10 anything. In some cases, it is I do not believe you. In  
11 some cases, it is that is not the role of the federal -- you  
12 saw this play out in, for example, some States' response to  
13 the election --

14           Senator Gillibrand: Correct.

15           Admiral Rogers: -- where some States came back and  
16 said, hey, look, that is your guys' role.

17           Senator Gillibrand: And that is the testimony we have  
18 heard in a few hearings now. So I am highly concerned that  
19 if you do not have the authority or some aspect of the  
20 Federal Government does not have authority to say to a  
21 secretary of state, we recognize it is a State's right to  
22 run elections. We recognize that you chose the technology  
23 that you want to pursue. We recognize this is a States  
24 rights issue. But if you do not have a level of  
25 sophistication that has been certified as cyber-protected,

1 it is not adequate.

2 So what I really hope you can come to this committee  
3 with is a list of authorities you might need to put in place  
4 before the next election because it is not adequate to defer  
5 this to any secretary of state in any given State that they  
6 think they are covered. We need assurances that they are  
7 covered by the most highly sophisticated cyber experts in  
8 our government. And I think a lot of that cyber expertise  
9 is being developed by the Department of Defense.

10 Admiral Rogers: Yes, ma'am.

11 Senator Gillibrand: But I think your leadership and  
12 coordination is so necessary.

13 Admiral Rogers: Yes, ma'am. Please, I do not dispute  
14 that at all. Much of what you are asking me, though, really  
15 falls under the Department of Homeland Security, and I do  
16 not want to speak for DHS because Secretary Kelly should be  
17 able to speak for himself.

18 I do acknowledge, particularly if we were to define  
19 this as critical infrastructure, clearly DOD has a role  
20 here.

21 Senator Gillibrand: Agreed.

22 Admiral Rogers: There is no doubt about that. Yes,  
23 ma'am.

24 Senator Gillibrand: With regard to the most recent  
25 French election, we saw that in that election emails of the

1 successful French candidate, Emanuel Macron, were dumped  
2 online after a previous hacking. There was also a rumor of  
3 campaigns launched against him on the Internet, and the head  
4 of the German domestic intelligence agency accused Russia of  
5 hacking the Bundestag in preparation for Germany's upcoming  
6 presidential elections.

7 How can the United States leverage our cyber and other  
8 capabilities to prevent Russian interference in not only our  
9 elections but those of allies and partners? And should we  
10 have a role? And what capabilities does CYBERCOM bring to  
11 the table to help deal with these type of threats?

12 Admiral Rogers: So this is much more in my role as the  
13 Director of NSA than Cyber Command.

14 But if you take a look at the French elections, for  
15 example -- again in an unclassified hearing, I am not going  
16 to get into specifics. But we had become aware of Russian  
17 activity. We had talked to our French counterparts prior to  
18 the public announcements of the events that were publicly  
19 attributed this past weekend and gave them a heads-up, look,  
20 we are watching the Russians. We are seeing them penetrate  
21 some of your infrastructure. Here is what we have we seen.  
22 What can we try to do to try to assist?

23 We are doing similar things with our German  
24 counterparts, with our British counterparts. They have an  
25 upcoming election sequence. We are all trying to figure out

1 how can we try to learn from each other, and that is much  
2 more my NSA role than in my Cyber Command role.

3 Senator Gillibrand: Thank you, Admiral.

4 Admiral Rogers: Yes, ma'am.

5 Chairman McCain: Senator Fischer?

6 Senator Fischer: Thank you, Mr. Chairman.

7 Thank you, Admiral, for being here today.

8 As you know, there has been some debate about our use  
9 of a geographically based counterterrorism strategy where  
10 legal authorities to conduct operations depend considerably  
11 on where they take place. To what extent are your  
12 operations in cyberspace similarly dependent upon the  
13 declared areas of active hostilities?

14 Admiral Rogers: So that is an issue for us. Authority  
15 is often granted by a defined geographic space. The point I  
16 try to make to policymakers is the challenge in the cyber  
17 arena, the infrastructure -- let us take ISIS, for example--  
18 that ISIS might be using is not necessarily physically in  
19 Syria and Iraq, but is in other areas. We need to be able  
20 to have an impact on that. I apologize. I do not want to  
21 go into this broadly in an unclassified forum. But we have  
22 that challenge. Yes, ma'am.

23 Senator Fischer: Are you bound then by the limitations  
24 that are set forward in the presidential policy guidance?

25 Admiral Rogers: Oh, yes, ma'am. I have to meet

1 PPD-20, for example.

2 Senator Fischer: So when you are looking at that and  
3 we look at the interconnectedness of the nature of  
4 cyberspace, so what impact does that have on your  
5 operations? Do you have the necessary ability to meet the  
6 requirements of the combatant commanders, the geographic  
7 combatant commanders?

8 Admiral Rogers: Not as fast as I would like. Again, I  
9 am not going to get into the specifics in an open forum.

10 But some of the things we are doing against ISIS, this  
11 very issue came to a bit of a head. We were able to work it  
12 out through the interagency process, and we were granted the  
13 authorities to execute some of the ongoing activity that we  
14 are doing against ISIS that extends beyond the immediate  
15 physical environment of Syria and Iraq. But I am the first  
16 to acknowledge it was not the fastest process in the world.  
17 It was a very complete process I am the first to acknowledge  
18 that.

19 Senator Fischer: Do you have suggestions for any  
20 changes that Congress needs to make in order for you to  
21 respond --

22 Admiral Rogers: Before I go to Congress, I am trying  
23 to have a dialogue with my own immediate bosses about so  
24 what might such a framework look like, and I think I owe  
25 them time to come to their own conclusions first.

1           Senator Fischer: And I understand that that  
2 presidential policy from 2013 is being reviewed by the  
3 Department. Is that correct?

4           Admiral Rogers: Again, it is not a Department  
5 document. It is a presidential document.

6           Senator Fischer: Is the Department reviewing it?

7           Admiral Rogers: We are broadly looking at cyber  
8 authorities right now at large. Again, I provided an input  
9 to the Secretary with, hey, sir, here are my views on what  
10 are some of the things that we might want to look at.

11          Senator Fischer: So CYBERCOM is involved in that  
12 review. And based on your experience, where do you think  
13 improvements should be made?

14          Admiral Rogers: Well, the positive side for me is  
15 everything I am hearing from the current team is they  
16 acknowledge that the structures that are in place are not  
17 fast enough. That is a good step for me because I am not  
18 spending a lot of time in a debate. Now it is, okay, so  
19 what do we do. If you accept that premise, what should we  
20 do?

21          Again, because that is an ongoing topic of discussion,  
22 I would just rather not publicly get into this. I think I  
23 owe them the time for them to come to their conclusions,  
24 although they are reaching out to us. I have no complaints  
25 in that regard.

1           Senator Fischer: Do you anticipate that the Secretary  
2 will be bringing forward to this committee any conclusions  
3 that are made then?

4           Admiral Rogers: I do not know, ma'am. I do not want  
5 to speak for the Secretary.

6           Senator Fischer: Okay.

7           Admiral, in testimony before the House Armed Services  
8 Committee in 2015, you mentioned an unresolved question  
9 about applying, quote, DOD-generated capacity in the cyber  
10 arena outside the government in the private sector. Can you  
11 elaborate on this? Specifically, what type of capacities do  
12 you believe would be beneficial, and what kind of gaps are  
13 you trying to fill?

14          Admiral Rogers: So it goes to some of the points that  
15 many of you made already this morning about, for example, if  
16 we are going to defend critical infrastructure, DOD is going  
17 to execute a mission and defend critical infrastructure.  
18 One of the points I am trying to make is I do not want to  
19 show up in the middle of a crisis for the first time I have  
20 interacted with some of these sectors. Just my experience  
21 as a military individual teaches me discovery, learning  
22 while you are moving in contact with an opponent is a  
23 painful way to learn. Increased loss. It takes so much  
24 more time, and you are not effective and efficient.

25          The argument I am trying to make is building on the

1 sector approach with critical infrastructure, which I think  
2 is very sound, can we not create standing mechanisms where  
3 I, the DOD, DHS, the private sector can operate 24/7 and  
4 operate with, hey, so what are we all seeing out there.

5 Senator Fischer: Do you support the deployment of  
6 government sensing capabilities on the private sector?

7 Admiral Rogers: In a perfect world, what I would  
8 probably prefer would be could we create a structure where  
9 the private sector could share the -- because they are  
10 putting sensors, putting telemetry on their networks. Could  
11 you not share that with us rather than us go in and do it?  
12 My first recommendation would be could we not create a  
13 mechanism where we can take advantage of the investments and  
14 the capabilities the private sector is already making.

15 Senator Fischer: Can we do that now?

16 Admiral Rogers: In some areas, we do that now. But I  
17 want to make it much more institutionalized and much more  
18 real time for me anyway.

19 Senator Fischer: Thank you.

20 Thank you, Mr. Chairman.

21 Chairman McCain: Senator King?

22 Senator King: Thank you, Mr. Chairman.

23 The first question, Admiral, for the record. We have  
24 been having these hearings now for 4 years, and we talk  
25 about the problem and everybody is absolutely convinced that

1 this is a very serious problem. I would appreciate it,  
2 given the fact of the depth of your knowledge and the work  
3 that you do, if you could supply for the record the five  
4 things you think we should do. Talking about it is  
5 important, but action. What are the five actions? If you  
6 would think about it, have some of your smart people think  
7 about it, whether it is legislation or regulation or new  
8 relationships, communication, I think all of us would find  
9 that helpful. This is an echo of Senator Wicker's question  
10 earlier.

11 [The information follows:]

12 [COMMITTEE INSERT]

13

14

15

16

17

18

19

20

21

22

23

24

25

1           Senator King: Second, we talk about this. We talk  
2 about this, we have got to approach this with a whole-of-  
3 government approach. I really think the term should be  
4 "whole-of-society."

5           Admiral Rogers: Yes, sir.

6           Senator King: Because this is an odd situation where  
7 you have got government for sure, but the vulnerable  
8 elements are in the private sector, the electric grid, the  
9 financial system, the gas pipeline system. And we had a  
10 situation -- I think it was in 2011 -- where there was a  
11 cyber bill. It was regulatory. It would have applied to  
12 the private sector. It failed. There was great resistance  
13 in the private sector to a regulatory approach.

14           We do not ask the private sector to defend themselves  
15 against Russian bombs or missile attacks from North Korea.  
16 We do that. What about a system whereby we work with the  
17 private sector to assist them financially in installing the  
18 kind of defensive measures that might be important, and in  
19 exchange, they would get perhaps some limitation of  
20 liability. And of course, they would get free stuff. The  
21 question is how do we do that without them just taking their  
22 foot off the gas and not protecting themselves.

23           Admiral Rogers: I mean, certainly incentivizing  
24 behavior generally tends to produce better outcomes in our  
25 society than the penalization piece. It is a much broader

1 issue than me.

2 But I think the core point you raise is the point I was  
3 trying to make with Senator Fischer. Traditionally in our  
4 society, we often have very strong walls between what is a  
5 private function and what is a government function. And I  
6 think cyber shows that much of what we are seeing is a  
7 national security issue, and therefore, it requires a whole-  
8 of-nation approach to how we are going to handle this.

9 Senator King: Which involves new levels in creative  
10 thinking about how to interface between the government and  
11 the private sector because we could have a perfect  
12 government system, but if Wall Street goes down, it is going  
13 to be chaos.

14 Admiral Rogers: I agree.

15 Senator King: On the issue of policy, Senator Rounds  
16 and I supported an amendment that got into the National  
17 Defense Act last year that essentially said to the  
18 administration 180 days a report is due on military/non-  
19 military options available for deterring and responding to  
20 imminent threats. That date is coming, just to remind you.  
21 It is June 23rd by my calculation.

22 Admiral Rogers: It is in June. Yes, sir.

23 Senator King: And this is a way of trying to force  
24 what Senator McCain has talked about about the development  
25 of a cyber policy. And then the President has 180 days

1 after that to describe the actions carried out in cyberspace  
2 that may warrant a military response. We have got to get  
3 through this.

4 Admiral Rogers: I know OSD is working on it. They  
5 have the lead here. They will respond formally. We have  
6 been part of that process.

7 Senator King: Well, I am just delighted that that is  
8 being worked on because I think one of our big gaps when we  
9 talk about what do we need to do, a policy and a strategy,  
10 as the chairman has mentioned, is absolutely critical  
11 because right now deterrence does not work unless there is a  
12 strategy and unless we know about it.

13 Admiral Rogers: Yes, sir.

14 Senator King: Finally, I think as we talk about this,  
15 if you think about what the Russians did in 2016, there were  
16 really three components. One was hacking and leaking. The  
17 other was attempted hacking in terms of the voting system,  
18 which we have talked about, which I think is a very serious  
19 issue. But the other is information and the manipulation of  
20 information. That is very hard to get at, especially in a  
21 place that has the First Amendment.

22 I would suggest that one of the things we need to be  
23 thinking about -- and this is not necessarily in your  
24 jurisdiction -- is a heightened level of digital literacy in  
25 this country. People have to understand when they are being

1 misled and manipulated, and perhaps they need to be given  
2 tips on how to do that. My wife has a sign in our kitchen  
3 that says the most difficult thing on the Internet is to  
4 determine the authenticity of quotes, Abraham Lincoln.

5 [Laughter.]

6 Senator King: But we have got to be educated. Our  
7 public has to understand that this is a whole new level of--  
8 way of manipulating. There were all kinds of reports in the  
9 French elections that Macron had bank accounts in the Cayman  
10 Islands. It is not illegal to say he had them. But how do  
11 you defend themselves against that? And I just would urge  
12 you to be thinking about this. How do we educate our people  
13 to be more discerning when they read something incredible on  
14 the Internet?

15 Admiral Rogers: It is a brave new world out there in  
16 the information dynamic for all of us.

17 Senator King: And it is particularly challenging in a  
18 country that values free expression.

19 Admiral Rogers: Right.

20 Senator King: Thank you.

21 Thank you, Mr. Chairman.

22 Chairman McCain: Senator Rounds?

23 Senator Rounds: Thank you, Mr. Chairman.

24 Admiral Rogers, first of all, thank you for your  
25 service to our country.

1           Wearing two hats, what is the earliest date that you  
2 think CYBERCOM should be elevated to a combatant command?  
3 If there are criteria, would you share the criteria?

4           Admiral Rogers: This is an ongoing policy issue, so I  
5 am not going to get into the specifics. I think that is not  
6 fair to my bosses. My input has been this is something I  
7 think we can do in a reasonably short period of time, make  
8 the initial steps.

9           Senator Rounds: Is there a set of criteria that you  
10 would expect to be completed before such a move was made?

11          Admiral Rogers: We have identified the steps within  
12 the Department. We have identified the steps that we would  
13 need to take to elevate to a combatant command. So again,  
14 that is why I say I am confident we could do this in a very  
15 short period of time.

16          Senator Rounds: Could you share with the committee in  
17 terms of what some of those activities have to be?

18          Admiral Rogers: We have identified we need to shift  
19 current responsibilities from STRATCOM down to us. We need  
20 to make changes to the unified command plan, which is a  
21 document signed by the President of the United States. It  
22 is the formal document that actually outlines what combatant  
23 commanders exist, what their defined responsibilities are,  
24 if there is a geographic aspect to those responsibilities.  
25 We have got to make those changes. And then we have

1 identified investments in manpower as well.

2 Senator Rounds: There would be an advantage in some  
3 ways to having two separate organizations. While the  
4 information that would be shared perhaps would be shared in  
5 a different manner, the sharing of that information could  
6 continue on, but the activities of the two would be  
7 different.

8 Could you share a little bit about the positive side of  
9 making a move like that?

10 Admiral Rogers: So I am on record as saying that my  
11 recommendation to this process has been that -- and I did  
12 not believe this when I came into the job, but after about 6  
13 to 9 months, I came to the conclusion, being in the two  
14 jobs, the right answer in the long term is to separate the  
15 two. They will still remain closely aligned because Cyber  
16 Command and NSA will still continue to work in the same  
17 battlespace in many ways, so to speak. So it will still be  
18 a unique relationship, but in the long run, I think it is  
19 the right thing to do.

20 I have also said, look, there is a series of steps we  
21 need to take to make sure that each organization, as it  
22 shifts from the structure we originally created, is  
23 optimized to continue to achieve successful outcomes. There  
24 are some things we need to do particularly on the Cyber  
25 Command side, but it is all within reason to me. It can be

1 done within a reasonable period of time and a reasonable  
2 level of investment.

3 Senator Rounds: How do you classify the private sector  
4 critical infrastructure that is vital to the DOD mission?  
5 And what efforts is CYBERCOM undertaking to protect private  
6 sector critical infrastructure that is vital to the DOD  
7 mission? I am not talking about trying to classify all the  
8 other stuff.

9 Admiral Rogers: No, no. I understand.

10 Senator Rounds: But just the items that are critical  
11 to DOD activity.

12 Admiral Rogers: So we try to partner closely with the  
13 Defense Security Service and the Defense Cyber Crimes Center  
14 to make sure that those critical businesses and  
15 infrastructure that we, the DOD, count on have access to  
16 information. The TRANSCOM Commander and I spent a lot of  
17 time focused on this. How do we make sure that the --  
18 because he, in particular, his organization, not that it is  
19 unique to TRANSCOM. It is probably at a greater level where  
20 their mission execution day to day is so dependent on  
21 capabilities resident in the private sector. He has  
22 probably got a greater challenge here than most. We are  
23 talking about how can we speed up processes.

24 I would like to see over time can we create a different  
25 relationship. It is hard right now to deal direct because

1 of the law and the framework we have created over time. I  
2 would like to see if we could potentially look at how we  
3 might amend that so we could deal more directly with a  
4 specific set of companies that have a direct relationship or  
5 provide a unique set of capabilities or infrastructure for  
6 DOD. I am working that with TRANSCOM.

7 We have also picked, in a couple places, Hawaii and  
8 Guam, for example, that are a little more isolated where it  
9 is a little easier, a couple test cases on how we can  
10 partner between the DOD and critical infrastructure on the  
11 islands, power and a few other things to highlight how do we  
12 work together very closely because there is no alternative  
13 generator capability, for example, off island that we are  
14 going to pipe in power. If we have problems with the power  
15 on the island distribution system, we got major problems for  
16 DOD.

17 Senator Rounds: I think sometimes we forget just how  
18 critical these cyber aspects are, and when we talk about the  
19 different domains that we fight in, air, land, sea, space,  
20 and cyber.

21 Can you think of any of the other areas that we require  
22 dominancy of that we would maintain dominancy in if we do  
23 not have dominancy in cyber?

24 Admiral Rogers: Well, it is one of the comments I made  
25 in my verbal opening statement. We not only are our own

1 mission set, so to speak, but our success helps to underpin  
2 the ability of the rest of the Department. I am not saying  
3 it is the only determinant, but it is a foundational element  
4 of the Department's broader ability to execute its mission  
5 sets across the breadth of DOD missions.

6 Senator Rounds: Thank you, sir.

7 Thank you, Mr. Chairman.

8 Chairman McCain: Senator Heinrich?

9 Senator Heinrich: Thank you, Chairman.

10 Welcome back, Admiral Rogers.

11 It has become really evident to me as a member of both  
12 the Intel Committee and this committee -- it has become  
13 crystal clear that Russia has really mastered this domain of  
14 digital disinformation and that they have effectively set up  
15 a situation where they are coordinating paid trolls, fake  
16 automated social media accounts, bots, as they call them,  
17 and state-backed news outlets to really amplify stories very  
18 effectively that serve their interest. And that is true of  
19 what we would call fake news. It is also true of any real  
20 news that simply serves their interests or undermines U.S.  
21 policy.

22 So these capabilities are proving to be just as  
23 politically disruptive both in our elections and day-to-day  
24 business, as well as what we have seen in Europe, as to the  
25 Russian hacking that we have seen.

1           So does Cyber Command have a role to play in meeting  
2 this new what I would describe as a threat, not just a  
3 reality? Or do you see it as wholly outside your lane?

4           Admiral Rogers: I would not say it is wholly outside.  
5 There is a broader issue to me, and information is one  
6 aspect of it. If you look at, for example, the way the  
7 spectrum and the network world are converging, if you look  
8 at the way the information dynamic is playing out, one of  
9 the questions that we are trying to come to grips with  
10 broadly within the Department, although I will be the first  
11 to admit I am so focused right now on trying to execute the  
12 missions I have been assigned -- part of my input to this  
13 process has been let me get the structures set before we  
14 start throwing more stuff on the life raft.

15           But I am trying to conceptualize in my own mind, so how  
16 are we going to bring together electronic warfare, cyber,  
17 and the information dynamic because it is all blurring in  
18 this digital world that we are living in. And how do we do  
19 this in an integrated way? And right now, we are not there  
20 yet. We are still trying to figure out what is the right  
21 way forward.

22           Senator Heinrich: Do you have people assigned to look  
23 at, for example, just the issue of when you have thousands  
24 and thousands of bots out there and they serve as a forcing  
25 mechanism, they look like social media accounts in Wisconsin

1 or Michigan or somewhere else in the United States, but they  
2 are really just automated accounts that take a story that  
3 has interested 10 people and makes it look like it is of  
4 interest to 10,000. Suddenly it is on my social media feed  
5 or my news feed on my iPhone.

6 Have we looked at capabilities for simply making it  
7 clear, even to the companies whose platforms those are on,  
8 that those accounts are not genuine accounts? Because it  
9 seems to me if you take that amplification piece out, even  
10 if it is on a constant rolling basis, you would have a  
11 dramatically diminished impact from this.

12 Admiral Rogers: Yes, although there are couple points,  
13 if I could.

14 First, remember much of the scenario you just went  
15 through is about domestic and both as NSA and Cyber Command,  
16 we are focused largely -- NSA -- we are focused externally.  
17 Cyber Command we are largely focused externally. So I will  
18 monitor bots infrastructure external to the United States.  
19 When it comes to --

20 Senator Heinrich: Well, bot farms typically are  
21 overseas. However, they are appearing to be domestic  
22 accounts but they are not attached to actual people in the  
23 United States.

24 Admiral Rogers: But one of the phenomena we are  
25 starting to see is you are certain to see a migration of

1 capability from the external infrastructure that we have  
2 been aware of and observing for some period of time. The  
3 way this is going to go next in my opinion, you are going to  
4 start to see this in domestic manipulation. And that is a  
5 part that for us right now, no, I am not really directly  
6 involved in.

7 We do, as part of the broader government effort  
8 participate in generating insight that we share with major  
9 social media providers to say, hey, this is activity that we  
10 are seeing that we believe to be false or that we believe to  
11 be criminal or we believe to be supporting of particular  
12 groups that are a threat to the Nation.

13 Senator Heinrich: So you are actually able in  
14 relatively real time to share information with big social  
15 media providers.

16 Admiral Rogers: In some cases, and I would not argue  
17 that it is necessarily immediate real time because one of  
18 the things that I try to do is kind of get a critical  
19 center-- get enough that I can try to show them a  
20 comprehensive effort here as opposed to coming to them with,  
21 hey, here is the count today, here is 10 the next hour  
22 because we are in the early stage of this. I am trying to  
23 engender a broader dialogue about, look, there is systematic  
24 here that both of us have got to be looking at. We got to  
25 stop looking at this one individual --

1           Senator Heinrich: Exactly. And I think it speaks to  
2 the relationship you were talking about. Whether you are  
3 talking about the financial services sector, the utility  
4 sector, or in this case, social media and media, we need to  
5 have those relationships in place to be much more responsive  
6 than we currently are.

7           Admiral Rogers: Yes, sir.

8           Senator Heinrich: Thank you.

9           Chairman McCain: Senator Ernst?

10          Senator Ernst: Thank you.

11          Admiral Rogers, it is good to see you again.

12          During Senator Fischer's line of questioning, you had  
13 answered that you do not want to show up in the middle of a  
14 conflict, you do not want to have to learn about the enemy  
15 on the move. And I agree. And I would also say that  
16 conversely we also want to know about our friendlies, and we  
17 do not want to learn about them on the move either.

18          So going back to the National Guard, we have  
19 corresponded back and forth a number of times. And we want  
20 to make sure that you know about those friendlies and the  
21 capabilities that they bring into your organization, should  
22 they ever be needed. So I did drop a bill earlier this year  
23 to ensure that DOD will start tracking these capabilities.

24          But from your perspective, what more can we be doing to  
25 help CYBERCOM connect with our National Guard and their

1 capabilities? What else can we do?

2 Admiral Rogers: So I feel pretty good about knowledge  
3 and awareness. I never thought as a commander -- but I can  
4 walk you through what Kansas is doing, Pennsylvania is  
5 doing, Delaware, Virginia, Washington, California. Again,  
6 it is kind of interesting to me. I think to myself, wow,  
7 Rogers, you are in a very different world here.

8 The biggest challenge that I am still trying to work --  
9 and it is one I have outlined about six different priorities  
10 for Cyber Command for calendar 2017. I said, hey, these are  
11 six things we are going to focus on. One of the six is  
12 about creating a model for Reserve and Guard integration.  
13 So I am trying to partner with Northern Command, as well as  
14 the National Guard Bureau, General Lengyel and his team,  
15 about, okay, so we are seeing the investments that the Guard  
16 and the Reserve is making, which I am very supportive of and  
17 appreciative of. Now, how do we create the mechanisms so we  
18 can actually apply that in real time?

19 We are doing some things now, for example, where Air  
20 Force is activating -- and in fact, I have reviewed the  
21 activation sequence in the Guard out to fiscal year 2020 for  
22 the Guard units we are going to bring on in active status to  
23 meet the requirements that the Air Force has for the Cyber  
24 Mission Force that I command, I lead.

25 But what I am trying to get to is if we have a major

1 cyber event, I feel very comfortable about we understand who  
2 is going to do what. What I am curious about is what  
3 happens if it is not something catastrophic, if it is not  
4 something that necessarily trips a threshold where the DOD  
5 active force is viewed as the primary responsibility. But  
6 how do we use those Guard and Reserve capabilities in  
7 instances where the active side is not necessarily going to  
8 be the lead? How do we make sure the capabilities are  
9 there? How do we apply them? What is the command and  
10 control structure that is in place?

11 We do that now in terms of defense support to civil  
12 authorities. That is very mature in terms of how we respond  
13 to natural disasters. We have got a great process there.  
14 Support to FEMA, the Northern Command's role. I am trying  
15 to argue we got to spend a little more time on the cyber  
16 piece of this.

17 Senator Ernst: Absolutely. I would agree  
18 wholeheartedly. Maybe it runs parallel to our civil support  
19 teams where they provide backup in case of any sort of  
20 incident, the Super Bowl, and things like that. We always  
21 have them on standby. And as we look at major events and  
22 progression, whether it is elections or other significant  
23 events, throughout the year, we have those Guard  
24 capabilities.

25 Admiral Rogers: Can I make one other point? I

1 apologize. I did not mean to interrupt.

2 One of the other challenges in the Guard construct, the  
3 Guard's construct is a geographic construct based on the  
4 State.

5 Senator Ernst: Yes.

6 Admiral Rogers: And so one of the challenges, again, I  
7 am trying to work my mind through -- and I had this  
8 discussion with the Council of Governors and the TAGs. In  
9 many instances, the infrastructure that a State is going to  
10 be counting on from a cyber perspective in the cyber arena  
11 does not necessarily physically reside in the State. So how  
12 do we take advantage of the Guard structure more broadly and  
13 not just -- I am not saying that the State piece is not  
14 important, but I am trying to figure how do we overlay a  
15 largely geographic and State-defined construct on something  
16 that is not always defined by immediate geography, if that  
17 makes sense.

18 Senator Ernst: It does make sense. It absolutely does  
19 make sense.

20 And I know a number of my colleagues, moving on to a  
21 different topic, have talked about personnel and how do we  
22 keep personnel there. So there have been a lot of  
23 suggestions about bringing civilians in to fill in the gaps.

24 But during Secretary Mattis' confirmation, he also  
25 stated that the warrior ethos is not a luxury. It is

1 essential when you have a military. And as we look at  
2 things like lateral accessions and flexible career paths,  
3 how do we make sure that warrior ethos is not being diluted?

4 Admiral Rogers: I am the first to admit. It is one  
5 reason why I have argued be leery of creating a cyber force  
6 that is predominantly civilian. No disrespect to my  
7 civilian teammates. But we want that warrior ethos and  
8 culture. Secondly, in the law of armed conflict, there were  
9 things legally that a uniformed military member of a nation  
10 state can do that a civilian cannot within a legal  
11 framework.

12 So civilians play an important role here. Do not get  
13 me wrong. And that is one of the reasons why I believe that  
14 the right construct for us is to bring the total spectrum,  
15 active, Guard, Reserve, contractor, civilian, private  
16 sector. It is our ability to bring it all together, not one  
17 single slice. So I would be leery about swinging the  
18 pendulum too far in one direction away from the military  
19 piece of that.

20 Senator Ernst: Thank you for laying that out. I  
21 appreciate your time, Admiral Rogers.

22 Thank you, Mr. Chair.

23 Chairman McCain: Senator Hirono?

24 Senator Hirono: Thank you, Mr. Chairman.

25 The Office of the Director of National Intelligence

1 released an intelligence community assessment on Russian  
2 activities and intentions in recent U.S. elections. And  
3 General Clapper testified regarding this report yesterday in  
4 the Judiciary subcommittee.

5 So we all know that Russia interfered with our  
6 elections. So do you view President Putin's actions in this  
7 regard as a cyber attack?

8 Admiral Rogers: Again, ma'am, that is a legal and a  
9 policy discussion. My point is it should be viewed as  
10 unacceptable. That is the bottom line to me. This is not a  
11 behavior you want to encourage. This is not a behavior we  
12 want to accept, nor is this a behavior I think we want to  
13 see repeated.

14 Senator Hirono: I think we all share that. How to get  
15 there is the challenge.

16 What is your opinion of the role of the military and  
17 intelligence agencies in preventing these types of events in  
18 the future?

19 Admiral Rogers: So, first, from an intelligence  
20 perspective, our job, speaking as the Director of NSA, is to  
21 generate insights and knowledge that help inform potential  
22 response and the ability also, if we can get ahead of the  
23 problem, to identify it in advance, intent, a nation where  
24 actors intend to do something, that then alarms policymakers  
25 and military commanders with the ability to engage in

1 operations or choices that clearly communicate to that other  
2 party, hey, we know what you are thinking about doing. You  
3 do not want to go down this road.

4 On the Cyber Command side, again, if we define election  
5 infrastructure as critical infrastructure to the Nation and  
6 we are directed by the President or the Secretary, I can  
7 apply our capabilities in partnership with others, because  
8 we will not be the only ones, the Department of Homeland  
9 Security, the FBI. I can apply those capabilities  
10 proactively with some of the owners of these systems.

11 Senator Hirono: It was very clear by General Clapper  
12 yesterday that Russia will continue these efforts. And in  
13 fact, we know that they have been doing this since the 1960s  
14 or 1970s, but it is just that they have many more tools in  
15 their toolbox to interfere with our elections. So you are  
16 still awaiting direction from the President for everyone to  
17 coordinate their efforts to stop this kind of behavior on  
18 Russia's part?

19 Admiral Rogers: No. I am saying I do not have a  
20 defined mission here. No one has changed that yet.

21 Senator Hirono: We need to do that for everybody to  
22 come together. Thank you.

23 The services continue to increase cybersecurity  
24 capabilities and develop advanced tools to combat cyber  
25 attacks. And PACOM has placed a focus on advanced cyber and

1 anti-satellite capabilities. How does CYBERCOM work with  
2 the other combatant commands like PACOM to counter the cyber  
3 threats they face?

4 Admiral Rogers: So I partner with -- I was just in  
5 Honolulu 2 weeks ago with Admiral Harris and his team  
6 sitting down and going, hey, because I try to get out there  
7 about -- for example, Hawaii, just an example. I am there  
8 generally every 6 months. I try to do this with all the  
9 combatant commanders everywhere around the world, sit down  
10 face to face with where are we, are we meeting your  
11 requirements.

12 Cyber Command in many ways -- much of what we do  
13 functions to support others. We exist to support and enable  
14 the success of others. So I always tell our team much of  
15 our success is going to be defined by others, not by us, and  
16 that is the way it should be. And so we spend a good deal  
17 of time aligning capability to meet specific combatant  
18 commander requirements, working with the combatant  
19 commanders as to what should be the priority for how those  
20 capabilities are applied. In many instances, I want them to  
21 set the priority not me. I have an opinion that we will  
22 partner together. And so, for example, that is what we are  
23 doing now in the Pacific from both a defensive and an  
24 offensive side.

25 Senator Hirono: And in your meetings with the other

1 combatant commands, then is part of your function to  
2 encourage -- to make sure that we do not have unnecessary  
3 duplication of effort across the services?

4 Admiral Rogers: So I try to make the argument, cyber  
5 is a high-demand/low-density capability, just like ISR, just  
6 like SOF, just like ballistic missile defense. And  
7 therefore, the same kinds of processes that we put in place  
8 to make sure we are maximizing the finite capability we  
9 have, we have got to do the exact same thing in cyber.

10 Senator Hirono: We know that we have challenges facing  
11 military recruiters in attempting to fill their cyber-  
12 related billets as other government agencies and the private  
13 sector try to fill their requirements as well. I would like  
14 to know specifically how important is it to continue non-  
15 military federal investments in education, particularly in  
16 the STEM programs, for American youth in order to meet the  
17 growing need of Cyber Command and other --

18 Admiral Rogers: Right. So as I said, our workforce is  
19 going to be a spectrum from the active, the Guard and  
20 Reserve, civilian, and contractors. For the civilian  
21 contractor and much of that active piece, much of this  
22 education is going to be done by the private sector, not by  
23 the government. So it is one reason why, as I said, we have  
24 relationships, if my memory is right, with over 200 academic  
25 institutions. It is one reason why I spend a fair amount of

1 time as a senior commander going to universities around the  
2 United States about so how are we going to create the human  
3 capital of the future in this. It is one reason why I spend  
4 a lot of time talking to the private sector about so tell me  
5 how you generate a workforce. How do you retain it? I  
6 acknowledge that there are some differences, but are there  
7 some things I could learn from you about what works for you?  
8 Because it cannot be all about money.

9 Senator Hirono: Thank you for that proactive posture.  
10 Thank you, Mr. Chairman.

11 Chairman McCain: Senator Tillis?

12 Senator Tillis: Thank you, Mr. Chair.

13 Admiral Rogers, it is good to see you again. You have  
14 been on the job about 2 years. Right?

15 Admiral Rogers: 3 years, sir.

16 Senator Tillis: 3.

17 Admiral Rogers: Yes, sir.

18 Senator Tillis: If you were to go back 3 years ago and  
19 you were in the same committee hearing, would the answers  
20 have changed substantially in terms of our current -- where,  
21 in other words, have we made significant progress?

22 Admiral Rogers: Where we made significant progress, we  
23 have capability. We are actually using it. We have got a  
24 good way ahead. We have got a commitment to that way ahead.  
25 So that is what I would have said as we --

1           Senator Tillis: But as you go through this, Admiral,  
2 if you think about looking at our near-peer competitors,  
3 they too are 3 years further along.

4           Admiral Rogers: Right.

5           Senator Tillis: So is the gap narrower or wider now  
6 between our capabilities to defend ourselves and to  
7 potentially respond to some attack?

8           Admiral Rogers: Narrowing. The gap is narrowing.

9           But to continue what I think was the point you are  
10 trying to make, but I would also tell myself, Rogers, you  
11 are not moving fast enough. We got to move faster. We got  
12 to prioritize. I am the first to acknowledge that. We are  
13 not where I want to be.

14          Senator Tillis: What about over the last 3 years, the  
15 sense of ownership in the private sector? I for one think  
16 we are making a huge mistake if we leave this hearing or if  
17 the private sector thinks we are coming up with a solution  
18 that they all benefit from. They are a part of an  
19 infrastructure that we cannot possibly be expected to --  
20 this is sort of like, you know, we are the police, back to  
21 Senator King's point. We have to respond when an attack  
22 occurs to try and figure out who did it and what the  
23 consequences should be. But we all need to have some sort  
24 of security ourselves in our businesses, in our homes, and  
25 our States. How well have they really improved over the

1 last 3 years since you have been in the position?

2 Admiral Rogers: It is uneven by sector. Some sectors,  
3 boy, have really made significant improvements; others, no.

4 To go to your point, the analogy I try to use, look, it  
5 is hard to expect the police force to stop burglaries if you  
6 are going to leave every one of your doors not just unlocked  
7 but open. You are going to turn all the lights on, and you  
8 are going to leave the house for an extended period of time.

9 Senator Tillis: And a sign saying "not at home."

10 Admiral Rogers: And just say -- right -- hey, feel  
11 free. That is not going to get us where we need to be.

12 Senator Tillis: Well, how do we move the ball? We had  
13 TRANSCOM in here for a hearing just last week or week  
14 before. How do we actually get to a point where we put  
15 pressure on the private sector not to mandate, but to maybe  
16 use it as a distinguishing factor when we are choosing  
17 between one potential contractor or supplier and another one  
18 in terms of the extent to which we believe that they are  
19 fully protected or protected as much as they can be in this  
20 space?

21 Admiral Rogers: So I think it goes to a combination of  
22 we need to change the basic contract language about it and  
23 set minimum expectations if you want to do business with the  
24 DOD.

25 Senator Tillis: Is that within your current

1 authorities?

2 Admiral Rogers: I am sorry, sir?

3 Senator Tillis: Is that within current authorities?

4 Admiral Rogers: Yes, and we have made some across the  
5 Department. We have made some changes in contractual  
6 language, but I think the evolution has shown us we got to  
7 be more specific.

8 Senator Tillis: To what extent is your command trying  
9 to -- in the discussion -- I think it was with TRANSCOM --  
10 we were talking about needing some sort of third party --  
11 there needs to be something out there to make sure that our  
12 suppliers, maybe even State agencies, are adhering to some  
13 baseline standards. To what extent is your command involved  
14 in that or who owns that?

15 Admiral Rogers: So we do not do that right now, but  
16 that is one of those changes I talked about, how do we  
17 change the relationship between DOD and its core private  
18 capability providers, infrastructure providers. Perhaps one  
19 of the things contractually you look at is so if you want to  
20 do business with us, you are signing up potentially to the  
21 idea that we can do an assessment, we can do an inspection.  
22 I think we need to work our way through that, but that is  
23 the kind of thing I think we need to be thinking about.

24 Senator Tillis: I think it is critically important.  
25 We have to also look at the reality that they have got a

1 supplier base, that the people that we contract with need to  
2 make sure they are holding their supplier base up to the  
3 same standard. I will just repeat what I always say in  
4 these committees. You can find a weaker link. All you can  
5 do is understand the supply chain and go after that one  
6 critical, seemingly innocuous component that shuts down your  
7 ability to repair a grid component or to repair some weapon  
8 in the supply chain.

9 In my remaining time, can you tell me a -- after  
10 elevation and the dual-hat split, how do you envision a  
11 standalone command operating? And what are the priorities?

12 Admiral Rogers: Well, again, now we are into a kind of  
13 "what if" scenario. So I would rather not go down -- I just  
14 do not like getting into "what if" kinds of things. That  
15 decision has not been made. That is a broader policy issue.  
16 I have had the opportunity to provide input to that process,  
17 but now we need to let the process play out and see what  
18 kind of bottom line the decision-makers come to. I just  
19 think that is fair and that is what we owe them.

20 Senator Tillis: Thank you.

21 Senator Reed [presiding]: On behalf of Chairman  
22 McCain, Senator Warren, please.

23 Senator Warren: Thank you.

24 I want to quickly ask about the importance of our non-  
25 military agencies and programs to your mission, which

1 includes defending the United States against cyber attacks  
2 by foreign and non-state actors. Our State Department  
3 promotes international norms of responsible behavior in  
4 cyberspace, and it helps make our partners and allies more  
5 cyber secure -- I think you have already talked about that  
6 some -- and counters online radicalization and recruitment  
7 by non-state actors like ISIS every day.

8 So, Admiral Rogers, you lead the best cyber warriors in  
9 the world. But I want to ask, would reductions in funding  
10 to the State Department's cybersecurity and counter  
11 radicalization programs make your job easier or harder?

12 Admiral Rogers: Tougher.

13 Senator Warren: I agree. I am concerned about the  
14 significant reductions to non-DOD departments proposed by  
15 the administration. These agencies provide critical support  
16 for your work, and I just want to make sure that does not  
17 get overlooked.

18 What I also want to do is follow up on a question that  
19 Senator Hirono asked. Last year, the Russians stole private  
20 emails and splattered them all across the Internet to help  
21 their preferred American presidential candidate. Last week,  
22 the Russians did exactly the same thing in order to help  
23 their preferred French presidential candidate. The United  
24 States of America needs to step up its game here. And I  
25 know that you are a key part of that.

1           Now, you stated in your prepared testimony, Admiral,  
2           that improving DOD's network defenses and building a  
3           cybersecurity culture depend on skilled people. So I would  
4           like to press you on the question of how we recruit and  
5           retain cyber warriors. Admiral, let me see if I can do this  
6           the right way.

7           We had a hearing recently in our military personnel  
8           subcommittee, and one of the witnesses said that the  
9           military recruiting system is so focused on filling quotas  
10          that they end up recruiting only for the military of today,  
11          not targeting the best suited to execute the missions that  
12          we are going to need a decade from now.

13          So, Admiral, can you tell us about your recommendations  
14          to ensure that we are recruiting the right talent for the  
15          cyber jobs and threats that we will face tomorrow?

16          Admiral Rogers: So my experience to date -- knock on  
17          wood -- has been I am very happy with the quality of  
18          individuals that we are seeing.

19          Senator Warren: I understand.

20          Admiral Rogers: We are exceeding retention broadly on  
21          the uniformed side. I have got a little more concern on the  
22          civilian side actually right now in terms of retention,  
23          particularly on the NSA side of my responsibilities.

24          The thing that is helping us at the moment is this  
25          workforce views themselves as the digital warriors of the

1 21st century, and their self-image is we are on the cutting  
2 edge of something brand new and every day we are shaping the  
3 future in a way that nobody else gets to do. And we are  
4 doing things that nobody else on the outside gets to do.  
5 They are empowered by the mission. And I am not going to  
6 pretend their leadership is perfect. But my sense is they  
7 think we got a focus, we got a vision, and we are driving  
8 it.

9       So I am constantly as a leader looking for what are the  
10 indicators if that is changing, how do I get ahead of this,  
11 and then what are the skill sets that I need not today but  
12 maybe 2 years from now, maybe 5 years from now.

13       Data is one area I would highlight. I am sitting here  
14 saying to myself right now we are probably not optimized for  
15 the data requirements of the near term. So what kind of  
16 data skills do I need? Is that a uniformed skill? Do I  
17 look at civilians to do that? Would a contractor make more  
18 sense? Is that something that the Reserves could do because  
19 they can put people in a skill set, and then, boy, they are  
20 going to stay there and do that? That is probably an  
21 example of where I am saying to myself maybe we need to be  
22 looking at -- it is still in my mind. We have not developed  
23 a formal plan, so to speak.

24       Senator Warren: But I am glad to hear it. You are  
25 looking out. I love the focus on data, you know, critically

1 important here.

2 In the 2017 Defense Department authorization, we gave a  
3 lot of flexibility on how to recruit talent specifically.  
4 So let me just ask, do you have all the authorities you  
5 need, or do we need more exemptions, for example, from  
6 federal hiring laws and other changes in the system to help  
7 you in your recruiting efforts not just today but 6 months  
8 from today and a year from today and a few years from today?

9 Admiral Rogers: Well, right now I feel good about  
10 military recruitment. I find our ability to hire on the  
11 civilian side -- we are lagging. And part of this is I tell  
12 our team is this something we are failing to understand. Do  
13 we have a lack of knowledge of our own system that we are  
14 not optimizing the system to generate the outputs we need?  
15 I am not at a stage yet where I have decided the answer is I  
16 have to go ask for more authority, but I have told the team,  
17 look, if we come to the conclusion that we have to ask for  
18 more authority, guys, that is what we are doing. We have  
19 got to take advantage of the willingness of this committee,  
20 the Department to work with us when it comes to flexibility  
21 on the human capital piece.

22 Senator Warren: Good.

23 I know how much you have invested in our cyber military  
24 force and the mission force overall. You have made enormous  
25 progress. But I do hope you will let us know.

1 Admiral Rogers: Yes, ma'am.

2 Senator Warren: And let us know more in advance rather  
3 than later. It takes a little while to get things through  
4 around here. But let us know because if you need more  
5 flexibility, you should have more flexibility. Thank you,  
6 Admiral.

7 Admiral Rogers: Thanks.

8 Chairman McCain [presiding]: Senator Perdue?

9 Senator Perdue: Thank you, Mr. Chair.

10 Admiral, good to see you again. Thank you for  
11 everything.

12 In testimony we heard earlier this year, the Defense  
13 Science Board said -- and I quote -- for at least the next  
14 decade, offensive cyber capabilities of our most capable  
15 adversaries are likely to far exceed the United States'  
16 ability to defend key critical infrastructures. Do you  
17 agree with that from the Defense Science Board?

18 Admiral Rogers: I said broadly. Clearly things favor  
19 the offensive side. Part of our challenge is much of our  
20 infrastructure represents investments and decisions and  
21 priorities made decades ago, and they are not reflective of  
22 the digital world we find ourselves in today. And the cost  
23 of replacing that fixed infrastructure is huge. And so it  
24 is not likely that we are going to replace all of that  
25 infrastructure in the immediate near term. Just the scale

1 is just beyond the ability of our society or our Nation  
2 right now.

3 Senator Perdue: So we are primarily focused on  
4 defense, deterrence, and detection right now from your  
5 earlier testimony, even today in this written testimony. My  
6 question is, in an open hearing like this, is there anything  
7 you can tell us about what we are doing on the offensive  
8 side? Are we developing offensive capabilities as well?

9 Admiral Rogers: So we have acknowledged that we are  
10 developing offensive capabilities. We have acknowledged  
11 that we are employing those capabilities in the fight  
12 against ISIS. I apologize. I would just rather not get  
13 into the specifics.

14 Senator Perdue: I understand.

15 I would like to move over to the question of the day,  
16 and it is how do you stand up this force over the next few  
17 years. And training is a very major part of this, as you  
18 have said. Between 2013 and 2016, under CYBERCOM's  
19 supervision, the Office of the Secretary of Defense and the  
20 Joint Staff were supposed to come to an agreement on a joint  
21 federated training program funded by the services for the  
22 training of the Cyber Mission Force. Can you update us on  
23 the status of that agreement and where we stand today on  
24 that?

25 Admiral Rogers: So we will transition to that model in

1 2018. The initial outfit, if you will, of the Cyber Mission  
2 Force, using much of NSA's infrastructure -- we signed up,  
3 speaking now as the Director of NSA, to use much of NSA's  
4 structure, our schoolhouses, our National Cryptologic  
5 School, for example, to do much, not all, but to do much of  
6 the training associated with the initial build-out of the  
7 mission force. That build-out, full operating capability is  
8 due to be completed, and we are on track for 30 September  
9 2018. The agreement then was at that point responsibility  
10 for training and development, long-term sustainment of the  
11 force would transition to a service structure. We are on  
12 track to do that right now.

13 Senator Perdue: So does that mean that each service  
14 would be responsible for developing their own cyber  
15 warriors?

16 Admiral Rogers: So what happens is we have a mandated  
17 training standard by position, each service then oftentimes  
18 partnering. For example, right now there is Navy training  
19 in Pensacola that all the services use, for example, because  
20 we all then get together and say so given this single common  
21 standard, given this single, agreed-to qualification  
22 process, what is the best way across the Department to make  
23 this work. What service has the best capacity, best  
24 capability? How do we manage throughput broadly? That is  
25 the only way to maximize this.

1           Senator Perdue: You mentioned context earlier, which  
2 is why you do not favor a unified force.

3           Admiral Rogers: Right. I was thinking about an  
4 integrated cyber --

5           Senator Perdue: I understand. I get it.

6           So having some experience in large organizations, I am  
7 concerned about that tradeoff. There is a balance.

8           Admiral Rogers: Right. Yes, sir.

9           Senator Perdue: We are in a crisis stage right now --  
10 I think you would agree to that -- with regard to our  
11 ability to detect and deter at this point. I understand  
12 long-term the ideal might be to have the service because of  
13 the context dimension.

14           In the interim phase when we are in this crisis mode,  
15 though, do we have a sense that that might be  
16 counterproductive to our ability to stand up to the  
17 immediate threats?

18           Admiral Rogers: It would be difficult to do it today  
19 in a short term. That would take a long-term investment,  
20 significant structural, cultural changes. It is another  
21 reason why I would argue optimize the structures and the  
22 mechanisms that are in place. Now, we also got to hold them  
23 accountable. Do not get me wrong. You just cannot turn to  
24 them and say, well, just do what you always do. There has  
25 to be accountability and oversight.

1           But I am comfortable that the current approach is going  
2 to generate the outcomes we need, even as I acknowledge it  
3 is not moving as fast as I would like. And we got a huge  
4 mismatch between current capacity and capability, and what I  
5 know is the requirement. We are always in a tail chase.

6           Senator Perdue: You mentioned earlier that the history  
7 has been the extraction of data from the system, that  
8 hacking -- the primary motive from Russia and China,  
9 primarily state actors, has been the extraction of data.

10           In North Korea, we saw a little bit of a different  
11 attack where they went in and actually started placing what  
12 I would call a sleeper embedded code, whatever, for a bigger  
13 mega event later. Do we see a continuing growth in that  
14 type of activity? Have we seen any evidence of that in the  
15 U.S.?

16           Admiral Rogers: You do. You see every nation state  
17 engaged. They will penetrate a system. They will look to  
18 not just extract but study it, understand it, see where it  
19 connects to. Can they use this as a jumping off point to  
20 get to somewhere else?

21           One of the things we are always looking for is so if a  
22 system has been penetrated, has the actor manipulated,  
23 changed, amended a configuration so they can gain access  
24 separately now. That is one of the key things we always  
25 look for when we are trying to do mitigation once someone

1 has penetrated a system.

2 So it is the full spectrum. The simple answer is yes.

3 It is the full spectrum.

4 Senator Perdue: Have we seen any in the U.S., any  
5 evidence of that in the U.S.?

6 Admiral Rogers: I have seen nation states engaged in  
7 activity in the U.S. where they clearly are interested in a  
8 long-term presence, not just extracting data.

9 Senator Perdue: Thank you, Admiral.

10 Chairman McCain: Senator Peters?

11 Senator Peters: Thank you, Mr. Chairman.

12 And, Admiral Rogers, always a pleasure to see you and  
13 enjoy your testimony as always.

14 My question involves the U.S. semiconductor industry,  
15 which right now faces some major challenges. In addition to  
16 some fundamental technological limits that are being reached  
17 in that area, there has also been a concerted strategic push  
18 by China to reshape the market in its favor using industrial  
19 policies backed by over \$100 billion in government-directed  
20 funds. And with semiconductor technology critical to the  
21 operation of critical U.S. defense systems, I am very  
22 concerned that China's industrial policies pose a real  
23 threat to U.S. national security.

24 And although we have a range of tools, which you are  
25 very familiar with, to deal with this, the principal

1 mechanism to manage it is the interagency Committee on  
2 Foreign Investment in the U.S., or CFIUS. And within the  
3 DOD, as you know as well, NSA is a key contributor to the  
4 CFIUS national security assessment. DIA, the military  
5 services, the combat commands all have a role in this  
6 process as well.

7 But my question is considering CYBERCOM's leading role  
8 within the Department, how is the command postured to  
9 support the CFIUS process for potential foreign mergers and  
10 acquisitions that have perhaps significant implications for  
11 the DOD cyber mission?

12 Admiral Rogers: So we predominantly interact in the  
13 CFIUS process on the NSA side. But one of the implications  
14 I think for the future -- again, it is just one input I have  
15 tried to make to the new team is I think we need to step  
16 back and reassess the CFIUS process and make sure it is  
17 optimized for the world of today and tomorrow because I am  
18 watching nation states generate inside knowledge about our  
19 processes. They understand our CFIUS structure. They  
20 understand the criteria broadly that we use to make broader  
21 policy decisions about is an investment acceptable from a  
22 national security perspective. And my concern is you are  
23 watching some nation states change their methodology to try  
24 to get around this process.

25 Senator Peters: Do you feel that CFIUS is adequately

1 resourced and authorized to make the kinds of changes that  
2 you think we need --

3 Admiral Rogers: I am not smart enough because we are  
4 just one element in this process, and it is not something  
5 that the DOD at large or Cyber Command or NSA runs per se.  
6 But I do think we need to step back and ask that kind of  
7 question to ourselves. Just my gut just tells me that that  
8 is one of the things we need to be doing.

9 Senator Peters: I would like to turn back to some of  
10 the discussions that we have had related to the involvement  
11 of the private sector, which has to be intimately involved  
12 in any kind of security operations. And I know your teams  
13 have operated Cyber Guards, over the years, exercises. And  
14 the most recent on you were involved in, simulating an  
15 attack on the Northeast, attacks on gulf oil facilities,  
16 ports across California. All of these entities, of course,  
17 are privately owned and not part of the Department of  
18 Defense.

19 And a recent GAO study, looking at some of the prior  
20 exercises, cited concerns that large portions of the  
21 exercise take place in a classified forum which places some  
22 inherent limitations on public and private sector  
23 participation. And although the arrangement certainly is  
24 designed to protect sensitive plans and capabilities -- and  
25 we all fully realize the importance of doing that -- the

1 approach also may fall short in preparing participants for a  
2 real world cyber emergency, which potentially could be  
3 catastrophic.

4 So my question is, how are you balancing the need for  
5 security with the realities of a cyber threat landscape that  
6 may ultimately necessitate very broad support from uncleared  
7 citizens and entities?

8 Admiral Rogers: So it is one of the reasons we changed  
9 the structure of Cyber Guard over time and tried to bring  
10 more in the private sector. So if you look at the scenario  
11 that you talked about that we did last year in terms of we  
12 simulated activity directed against the power grid in the  
13 east, the petroleum industry in the gulf, and port sectors  
14 on the west coast. We went to several private companies  
15 within each of those sectors and said, hey, we would like  
16 you to participate in this. What do we need to make that  
17 happen?

18 We also increasingly are going to the private sector in  
19 terms of private sector companies that run the  
20 infrastructure associated with supporting those entities.  
21 We have added that to the Cyber Guard arena.

22 So I am trying to see can we create an exercise in  
23 addition. We do tabletop exercises, which are not quite --  
24 Cyber Guard is huge. It is like a thousand individuals.

25 We also do regular tabletop exercises where we talk at

1 a high level so we can skirt some of the security aspects of  
2 the classification aspects of this and bring in the private  
3 sector. We do that out at the Fort Meade complex several  
4 times a year separately from Cyber Guard.

5 Senator Peters: Thank you, Admiral.

6 Chairman McCain: Senator Cotton?

7 Senator Cotton: Thank you, Admiral Rogers. Welcome  
8 back.

9 I want to talk about Russia today and how they hacked  
10 into those emails and released them last year. I want to  
11 touch on that.

12 Specifically Senator Warren a few moments ago continued  
13 to refer to the President as Russia's preferred candidate.  
14 I think she is referring there to the intelligence community  
15 assessment of January 6th, primarily written by your agency,  
16 the NSA, along with the CIA and the FBI.

17 This brings to mind a curiosity from the report that I  
18 wanted to raise with you and ask about. In the key  
19 judgments, the report says we also assess Putin and the  
20 Russian Government aspired to help President-elect Trump's  
21 election chances, when possible, by discrediting Secretary  
22 Clinton and publicly contrasting her unfavorably to him.  
23 All three agencies agree with this judgment. CIA and FBI  
24 have high confidence in this judgment. NSA has moderate  
25 confidence.

1           Could you explain the discrepancy for us?

2           Admiral Rogers: I would not call it a discrepancy. I  
3 would call it an honest difference of opinion between three  
4 different organizations. And in the end, I made that call.  
5 So if anybody is unhappy, Mike Rogers is the accountable  
6 individual.

7           When I looked at all the data, I was struck by for  
8 every other key judgment in the report by multiple sources,  
9 multiple disciplines, and I was able to remove almost every  
10 other alternative rationale I could come up with in my mind  
11 for, well, could there be another reason to explain this.  
12 In the case of that one particular point, it did not have  
13 the same level of sourcing and the same level of multiple  
14 sources from different perspectives, you know, human  
15 intelligence, signals intelligence.

16           I still believe that it made sense. I still believe  
17 that it fit within the context, and I still agreed with the  
18 judgment. But I did say from a professional analytic  
19 perspective, I am not quite at the same confidence level as  
20 my two counterparts in the form of John Brennan and Jim  
21 Comey.

22           Senator Cotton: The one particular point being going  
23 from saying Russia wanted to hurt Secretary Clinton's  
24 chances, in addition help Donald Trump's chances.

25           Admiral Rogers: Correct.

1           Senator Cotton: Those are hard to disentangle --  
2 right-- since in our election system we have to first pass  
3 the post as long as you do not have a --

4           Admiral Rogers: In this case, there was some pretty  
5 specific intelligence that seemed to differentiate that  
6 there were specific thoughts on the part of the Russians on  
7 each of the aspects of that statement, if you will.

8           Senator Cotton: Obviously, we cannot discuss those  
9 classified matters, but there is a lot of open source  
10 matters as well. President Trump, for instance, was the  
11 candidate who wanted to build up our defenses, expand our  
12 missile defenses, accelerate nuclear modernization, pump  
13 more North American oil and gas. None of those things  
14 seemed to be very favorable to the Kremlin. Did your agency  
15 take those things into account?

16          Admiral Rogers: Yes, sir.

17          Senator Cotton: And also if you look back over the  
18 last 8 years, just a quick rundown of what I could recall --  
19 I am sure I am missing some -- the Obama administration in  
20 2009 reset relations with Russia 6 months after it invaded  
21 Georgia.

22                 2010, signed New START, which I would say was a better  
23 treaty for Russia than us.

24                 2012, in a hot mike moment with Dmitry Medvedev,  
25 President Obama said he would have more flexibility on

1 ballistic missile defense after his election. He also  
2 mocked his opponent at a presidential debate saying that  
3 Russia as our number one geopolitical foe.

4 2013 was the red line fiasco in Syria with Russia's  
5 closest Middle East ally when President Obama accepted  
6 Vladimir Putin's offer to remove chemical weapons from  
7 Syria, which we now know was a failed effort.

8 2014, we stood largely idly by during the Crimea  
9 invasion and did not offer defensive weapons when Russian-  
10 backed separatists started fighting in the Donbass despite  
11 bipartisan support from this committee. By that point, we  
12 had long since been ignoring INF Treaty violations that our  
13 military now acknowledges.

14 2015, Russia had a massive surge into Syria and  
15 continued its effort to block U.N. Security Council  
16 resolutions.

17 2016, they pummeled Aleppo into submission. In  
18 private, they objected to numerous provisions that I wrote  
19 in the Intelligence Authorization Act that would hold Russia  
20 to account in its espionage effort, and they increased the  
21 amount of times they are buzzing aircraft and warships in  
22 Europe and the Arctic.

23 President Trump promised to reverse those policies.  
24 Secretary Clinton largely campaigned on continuity. That  
25 does not sound to me like something that the Kremlin would

1 be happy about.

2 Admiral Rogers: I am just going by the intelligence.  
3 It was very clear in the intelligence of Russians'  
4 perceptions.

5 Senator Cotton: Do you think given that 8-year history  
6 of the Obama administration that Russian intelligence and  
7 leadership felt emboldened to undertake the hacks of those  
8 email systems and release them?

9 Admiral Rogers: Now you are into political judgment,  
10 sir, and that is just not my area.

11 Senator Cotton: Thank you very much.

12 Chairman McCain: Senator Kaine?

13 Senator Kaine: Thank you, Mr. Chair.

14 Just to follow up, Admiral Rogers, on this issue of  
15 moderate confidence, did you have a high degree of  
16 confidence that there was an effort to discredit one  
17 candidate and only a moderate degree of confidence that  
18 there was an effort to support --

19 Admiral Rogers: If you read the key judgments, what it  
20 says is I concurred in the report in the sense that we had  
21 high confidence in the judgment that the Russians clearly  
22 were trying to undermine our democracy and discredit us  
23 broadly, that they wanted to specifically make sure  
24 candidate Clinton did not win and to undercut her  
25 effectiveness should she have won.

1 Senator Kaine: High confidence in that.

2 Admiral Rogers: Right. High confidence in that and  
3 that it was just the last part about -- and their judgment  
4 was they wanted candidate Trump to win. And that was one of  
5 the objectives --

6 Senator Kaine: We had testimony in this committee  
7 probably a year and a half ago by General Dunford where he  
8 was asked the question I think by Senator Manchin which was  
9 the nation state that he would view as our most significant  
10 adversary. And he testified, based on their capacity and  
11 intent, he thought that would be Russia.

12 Just in your domain, cyber, the cyber domain, do you  
13 view Russia as an adversary? They have taken actions that  
14 have put them in the position as an adversary of the United  
15 States in the cyber domain.

16 Admiral Rogers: I am watching them engage in behaviors  
17 that I think are destabilizing and not in our best interests  
18 in cyber.

19 Senator Kaine: Would you also agree that France is an  
20 ally? They are a NATO ally and they are also a coalition  
21 partner in Afghanistan.

22 Admiral Rogers: Yes, sir.

23 Senator Kaine: You are aware of the reports in the  
24 last few days that there was significant evidence tying  
25 Russia to a hacking effort to destabilize the French

1 election. That is something we should take seriously when  
2 an adversary tries to destabilize the government of an ally.  
3 Would you agree?

4 Admiral Rogers: Yes, sir.

5 Senator Kaine: There was an article in the "New York  
6 Times" the day before the election, Saturday, the 6th, with  
7 a fascinating headline. "U.S. Far Right Activists Promote  
8 Hacking Attack Against Macron," and the article was about  
9 the effort by groups in the United States to immediate  
10 spread the hacked documents in many instances before even  
11 WikiLeaks was able to.

12 If we should take seriously an adversary's cyber attack  
13 on the democracy of an ally, should we be indifferent or  
14 concerned about efforts of Americans to work together with  
15 or in parallel with an adversary attacking the democracy of  
16 an ally?

17 Admiral Rogers: I apologize. I am not sure I am  
18 understanding.

19 Senator Kaine: You have testified in response to my  
20 question that we ought to take seriously if an adversary  
21 tries to cyber attack and destabilize the democracy of an  
22 ally. If American organizations are working together with  
23 or in parallel with an adversary --

24 Admiral Rogers: A foreign counterpart?

25 Senator Kaine: -- as they are trying to attack the

1 government of an ally France, should we be in different to  
2 that, or should we take that seriously as well?

3 Admiral Rogers: We need to be concerned.

4 Senator Kaine: Okay. And if we are concerned about  
5 that, if the U.S. Government should be concerned in this  
6 case -- and I will introduce this article for the record.

7 [The information follows:]

8 [COMMITTEE INSERT]

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

1           Senator Kaine:  If we should be concerned about the  
2  efforts of folks in the United States to work together with  
3  or in parallel with an adversary like Russia attacking an  
4  ally like France, where should that concern lie in the  
5  Federal Government?  Is that a law enforcement matter?  Is  
6  it a DHS matter?  Is it an NSA matter, or is it a Cyber  
7  Command matter?

8           Admiral Rogers:  I would argue it depends on the  
9  specifics of the scenario.  I am not trying to be  
10 dismissive, Senator.  It is a very complex question.

11          Senator Kaine:  And I will put the article in for the  
12 record, and there is, I think, more to come on this.

13          But if individuals or organizations in the United  
14 States, for example, were taking hacked documents from an  
15 illegal Russian hack of the French system and trying to  
16 disseminate it to affect the French election, this is  
17 something we should be concerned about.  Where would that  
18 concern lie within --

19          Admiral Rogers:  My first thought would be the FBI, but  
20 again, that is not necessarily a fully informed opinion, but  
21 it is the first thing that comes to my mind.

22          Senator Kaine:  All right.

23          Let me ask you this.  There has been some debate in the  
24 last couple of days about whether there is such a thing as a  
25 good shutdown of the United States Government.  Can you see

1 any circumstance under which Cyber Command's mission would  
2 be benefited by a shutdown of the Government of the United  
3 States?

4 Admiral Rogers: No. And if I could, I know you are  
5 asking for a yes or no. The number one issue that my  
6 workforce often raises with me is what we went through in  
7 2013, and it is now 4 years later. And I still -- every  
8 time there is the merest hint in the media of this even  
9 potentiality, I get, sir, are we going to go through this  
10 again, sir? You said this was not going to happen, sir. I  
11 thought they were committed to us and our mission. Sir, I  
12 do not want to work in an environment where every couple of  
13 years I am just getting jerked around about am I going to  
14 come to work, am I going to get paid, do they value what I  
15 do. Hey, sir, we just want to do the mission. We just need  
16 the support to keep moving forward.

17 Senator Kaine: Thank you, Admiral.

18 Thank you, Mr. Chairman.

19 Chairman McCain: Senator Graham?

20 Senator Graham: Thank you, Admiral. Thank you for  
21 your service.

22 Director Comey said a couple of days ago -- I guess it  
23 was last week in the hearing that I was involved in in  
24 Judiciary -- that Russia is still interfering in American  
25 politics. Do you concur with that?

1 Admiral Rogers: Yes.

2 Senator Graham: He also said that among nation states,  
3 he thought Russia had the most capability and the biggest  
4 intent in terms of interfering in the future. Do you agree  
5 with that?

6 Admiral Rogers: Yes.

7 Senator Graham: Do you agree that it was Democrats in  
8 2016? It could be Republicans in the next election?

9 Admiral Rogers: Yes. I would argue this is not about  
10 politics. This is not about party. This is about an effort  
11 against the strategic interests of every citizen of this  
12 Nation.

13 Senator Graham: I agree with you 1,000 percent.

14 Do you they agree they could do this in congressional  
15 races, House and Senate --

16 Admiral Rogers: Yes.

17 Senator Graham: Do you agree that if somebody does not  
18 make them pay a price, they are going to keep doing this?

19 Admiral Rogers: Yes.

20 Senator Graham: All right. Unmasking. A lot of talk  
21 about it. Are you aware of any incidental collection on  
22 2016 candidates on both sides of the aisle?

23 Admiral Rogers: I am not going to get into specifics  
24 in an unclassified forum about collection at large. But I  
25 will say we certainly acknowledge that incidental collection

1 occurs, but we also have a very strict process --

2 Senator Graham: Can we build that out a bit?

3 Admiral Rogers: -- for what we do with it.

4 Yes, sir.

5 Senator Graham: The only way you can actually collect  
6 on an American citizen inside the country is to have a FISA  
7 warrant.

8 Admiral Rogers: Get a FISA warrant. Yes, sir.

9 Senator Graham: Or if an American citizen is  
10 incidentally in a conversation with somebody you are already  
11 following.

12 Admiral Rogers: Yes, sir.

13 Senator Graham: Unmasking is a request to your  
14 organization, I want to know who American citizen 1 was.

15 Admiral Rogers: Yes, sir.

16 Senator Graham: How many of those requests did you get  
17 in 2016?

18 Admiral Rogers: I think we have publicly  
19 acknowledged --

20 Senator Graham: Around 2,000.

21 Admiral Rogers: 2,000. I think it is --

22 Senator Graham: How many people can request the  
23 unmasking of American citizens?

24 Admiral Rogers: If you are an authorized recipient of  
25 the intelligence, we use two criteria. Number one, the

1 requester must be asking this in the execution of their  
2 official duties. It cannot be something that would be need  
3 to know. Number one has to be in the execution of their  
4 official duties. Number two, the revealing of a U.S. person  
5 has to provide context and greater value for the  
6 intelligence. Again, it just cannot be I am just curious.

7 Senator Graham: I got you.

8 So within our government, are there 10 people -- 10  
9 groups that groups that can do this? 20?

10 Admiral Rogers: In terms of authorizing the unmasking?

11 Senator Graham: Yes. No, to make the request.

12 Admiral Rogers: No, it is broader than that. If you  
13 are on the distribution -- if you are on the authorized  
14 distribution for our intelligence reporting, you can ask.  
15 It does not mean it gets approved, but you can ask.

16 Senator Graham: Does the National security Director --  
17 one of those -- I mean --

18 Admiral Rogers: The National Security Advisor? Yes,  
19 sir. They are normally on the distribution for most, not  
20 all.

21 Senator Graham: Is there a record of every request  
22 made?

23 Admiral Rogers: Yes.

24 Senator Graham: So there is a record of who made the  
25 request to unmask the conversation involving the American

1 citizen.

2 Admiral Rogers: Yes, sir.

3 Senator Graham: There is a record whether or not you  
4 granted it.

5 Admiral Rogers: Yes, sir.

6 Senator Graham: Is there a record of what the person  
7 did with the information once they got it?

8 Admiral Rogers: No. There is also a record of the  
9 basis of, so why did we say yes. Remind every individual,  
10 if I could, once we unmask, once we authorize an unmasking,  
11 we authorize the unmasking only to that individual. What do  
12 I mean by that? So if we unmask a report that went to a  
13 particular individual, we do not unmask the report for  
14 everyone who got that report. Only the individual that  
15 we --

16 Senator Graham: And they are told not to share it  
17 with --

18 Admiral Rogers: And they are specifically told. This  
19 does not change the classification.

20 Senator Graham: General Flynn was caught up in a  
21 conversation with the Russian ambassador. You are familiar  
22 with that story in the press.

23 Admiral Rogers: I am familiar with the story. Yes,  
24 sir.

25 Senator Graham: Assuming he did not have a FISA

1 warrant allowing us to collect on him, it would be a case of  
2 incidental collection following the Russian ambassador.

3 Does that sense?

4 Admiral Rogers: Yes, sir.

5 Senator Graham: We would know how that conversation  
6 was revealed and to who it was revealed through the request  
7 of your agency.

8 Admiral Rogers: If we unmasked and it was based on an  
9 NSA report. Remember, NSA will not be the only agency that  
10 potentially could have gotten the conversation.

11 Senator Graham: Got you, but you are the primary one.  
12 Right?

13 Admiral Rogers: I would argue again it depends. If  
14 you look at Title 1 warrants, the FBI --

15 Senator Graham: I am not talking about warrants. I am  
16 talking about --

17 Admiral Rogers: Incidental. So I would argue there is  
18 probably a greater potential on the FBI side than NSA just  
19 generally in terms of collection.

20 Senator Graham: Of incidental collection?

21 Admiral Rogers: Incidental with U.S. persons.

22 Senator Graham: So we could either ask the FBI or you.

23 Admiral Rogers: Yes, sir.

24 Senator Graham: So somebody took that information that  
25 we gained through collection with Flynn and gave it to the

1 "Washington Post."

2 Admiral Rogers: Somehow it got to the media.

3 Senator Graham: That is a crime.

4 Admiral Rogers: And that is a leak, and that is  
5 illegal. Yes, sir.

6 Senator Graham: Are you concerned about people taking  
7 the law in their own hands no matter how noble they think  
8 the event would be?

9 Admiral Rogers: Oh, yes, sir, which is why I have gone  
10 to my workforce in writing and said let us make sure we  
11 understand what the professional ethos of our organization  
12 is. We do not -- if I could finish, sir. We do not engage  
13 in this behavior, and if I catch you engaging in this  
14 behavior, I will hold you criminally liable and you have no  
15 place --

16 Senator Graham: Mr. Chairman, can I ask for additional  
17 30 additional seconds?

18 The bottom line here, it is possible for the Congress  
19 to find out who requested unmasking of American citizens,  
20 who that information was given to, and that is possible for  
21 us to know.

22 Admiral Rogers: On the NSA side, that is part of the  
23 ongoing investigation with the primary oversight committees  
24 that we are going through right now.

25 Senator Graham: Do you know is Susan Rice ever asked

1 for an American citizen to be unmasked?

2 Admiral Rogers: I would have to pull the data, sir. I  
3 apologize.

4 Senator Graham: Thank you.

5 Chairman McCain: Senator Blumenthal?

6 Senator Blumenthal: Thanks, Mr. Chairman.

7 Thank you, Admiral Rogers, for being here again and  
8 thank you for your service.

9 We have heard repeatedly in this room, as well as  
10 yesterday with Director Clapper, that the Russians will  
11 continue attacking the United States unless they are forced  
12 to pay a price. And you agree.

13 Admiral Rogers: Yes, sir.

14 Senator Blumenthal: And right now, are they being  
15 forced to pay a price?

16 Admiral Rogers: Certainly nothing that is changing  
17 their behavior.

18 Senator Blumenthal: Nothing that is changing their  
19 behavior, and clearly nothing that will change their  
20 behavior in the future because, to quote you or paraphrase  
21 you, they have more to gain than to lose by continuing this  
22 kind of attack.

23 Admiral Rogers: Yes, sir.

24 Senator Blumenthal: So can you recommend to us what  
25 kinds of measures should be taken? And I know you have been

1 asked this question before. In fact, you were asked when  
2 you last testified here. And you said that tools like  
3 sanctions can be an effective option. But so far, the  
4 sanctions in my view are way less than they should be. Do  
5 you agree that sanctions can and should be increased to  
6 provide a price that the Russians --

7 Admiral Rogers: So now you are into a policy judgment.  
8 I will only say sanctions I think have proven to be an  
9 effective tool in many scenarios. I am not going to argue  
10 that they are perfect and they work all the time.

11 Senator Blumenthal: But there will be a point where a  
12 cyber response should be appropriate.

13 Admiral Rogers: Potentially although I would highlight  
14 when we think about deterrence, we need to think more  
15 broadly than just cyber. Just because someone comes at us  
16 in cyber, does not mean we should automatically default to,  
17 well, it has got to be an exact response in kind. I think  
18 we need to think more broadly and play to our broader  
19 strengths as a Nation.

20 Senator Blumenthal: There is no question that the  
21 Russians attacked this country through cyber. And would you  
22 agree that Americans who colluded or cooperated with that  
23 attack also should be held accountable?

24 Admiral Rogers: Broadly yes, but again, now you are  
25 starting to get into a legal and a policy piece, and that is

1 just not my lane in the road.

2 Senator Blumenthal: Well, your lane includes defending  
3 this Nation from cyber attack.

4 Admiral Rogers: Yes, sir. But not necessarily action  
5 against particular individuals.

6 Senator Blumenthal: Well, let us talk about a group of  
7 Americans who may have colluded or cooperated with the  
8 Russians in enabling or encouraging this kind of attack.  
9 And by the way, they violated criminal laws if they did so.  
10 Would you not agree that they should be held accountable and  
11 that an investigation of it is appropriate and necessary?

12 Admiral Rogers: So I agree an investigation is  
13 appropriate and necessary, and if they violated the law,  
14 then, yes, sir. I am just not an attorney. I am not a  
15 lawyer. I am not a law enforcement individual. It is not  
16 my area of expertise.

17 Senator Blumenthal: But unless they are made to pay a  
18 price as well, the Russians will be enabled and encouraged  
19 in the future.

20 Admiral Rogers: Yes, sir.

21 Senator Blumenthal: And they will be paying less of a  
22 price as well.

23 Admiral Rogers: Right.

24 Senator Blumenthal: I feel like we are in a time warp  
25 here because when you were last here, we agreed that we need

1 a policy and a strategy, as the chairman has articulated so  
2 well, and we still do not have one. Can you tell the  
3 American people whose responsibility it is to develop that  
4 strategy and policy?

5 Admiral Rogers: It is ultimately the executive branch.  
6 There are multiple components, but ultimately it boils down  
7 to the executive branch. As I have said, look, we have a  
8 new team in place. They are working their way through this.  
9 In fairness to them, this is not a -- this is a complicated  
10 topic with a whole lot of complexity and nuance. I know  
11 that these discussions are ongoing. I have been a part of  
12 some of them. I am grateful that the team is willing to  
13 reach out and say, hey, Admiral Rogers, from your  
14 perspective, what do you think, what do you see, what are  
15 you thinking about. So I do not want anybody walking away  
16 thinking nothing is going on, no one is thinking, they are  
17 not attempting to proactively try to grapple with these very  
18 tough problems.

19 Senator Blumenthal: Well, I just want to conclude by  
20 stressing again that forcing the Russians to pay a price for  
21 their attack on this country requires compelling Americans  
22 who colluded or cooperated with them to pay a price, but  
23 also a strategy and policy for knowing when there is a cyber  
24 attack on this Nation, when it is an act of war that should  
25 prompt a response in the cyber domain or in other military

1 domains and economic sanctions that also may force them to  
2 pay a price. And right now, our policy of deterrence is in  
3 my view an abject failure.

4 Admiral Rogers: Not achieving the desired result.  
5 That is clearly true. Yes, sir.

6 Senator Blumenthal: Thank you.

7 Thanks, Mr. Chairman.

8 Chairman McCain: Senator McCaskill?

9 Senator McCaskill: Thank you, Mr. Chairman.

10 Good to see you, Admiral. Thank you for your service.

11 We have heard over and over again in multiple hearings-  
12 - and we have got our cyber hearing in Homeland Security  
13 tomorrow. So this is really timely for me -- about poor  
14 information sharing and understanding the challenges of  
15 classified information.

16 My staff has tried to chart the national cybersecurity  
17 structure for me. And the one thing that sticks out to me  
18 is this cyber unified coordinated group. It appears to me  
19 to be really the only place that our structure is set up  
20 under PPD-41 where the private sector entities really seem  
21 to plug into the national structure. The interesting thing  
22 is this cyber unified coordinated group is supposed to be in  
23 response to a significant cyber event. That is the  
24 operative phrase.

25 In the United Kingdom, the NCSC has real-time

1 collaboration with emphasis on exchange of classified  
2 information on an ongoing basis.

3 My first question for you is has the cyber unified  
4 coordinated group ever been called into a session. Has  
5 there ever been ongoing meetings? Have there been any  
6 meetings of this particular group that is laid out in  
7 PPD-41?

8 Admiral Rogers: It does interact. It does operate. I  
9 would be the first to admit, ma'am, I have to take the  
10 question for the record about has it ever physically met.

11 We participated in it, and I am trying to remember if  
12 it is done. Some of the work we do virtually. We will take  
13 an issue and we will do it via email and video conference.  
14 If I could, if you would like, I can take that for the  
15 record.

16 [The information follows:]

17 [COMMITTEE INSERT:]

18

19

20

21

22

23

24

25

1           Senator McCaskill: Yes, because I am trying to think.  
2           It seems to me like to me the Russian thing is a significant  
3           cyber event. And I guess my problem is with this, I know we  
4           have spent a lot of time today struggling about what our  
5           policy is. It looks like to me that we do not really have  
6           anywhere where there is an ongoing meeting structure that  
7           integrates the private sector into what is a pretty  
8           convoluted setup that we have right now.

9           Admiral Rogers: Could I disagree slightly, if I could?

10          Senator McCaskill: Sure.

11          Admiral Rogers: I think it is fair to say that at a  
12          sector level we do have constructs that enable that to  
13          occur. But one of the things the hack points out -- for  
14          example, the Russian influence effort points out is we do  
15          not have a sector labeled U.S. election infrastructure like  
16          we do in power, like we do in transportation.

17          Senator McCaskill: Although DHS has named election  
18          infrastructure as part of their critical infrastructure --

19          Admiral Rogers: Right, now.

20          Senator McCaskill: -- responsibility.

21          Admiral Rogers: Yes, ma'am. Now.

22          Senator McCaskill: And that happened last year maybe  
23          in response to this. I hopefully will find out more  
24          tomorrow.

25          I guess it seems to me that when someone is impacting

1 our elections, that overlooks all because if you look at  
2 this list, our national policies certainly impact chemical,  
3 commercial, communications, manufacturing, dams, I mean  
4 everything gets impacted.

5 Admiral Rogers: Right.

6 Senator McCaskill: Forget about Russia for a minute.

7 Are you familiar with the UK model?

8 Admiral Rogers: Yes, ma'am, very much so.

9 Senator McCaskill: So why are we not doing that? What  
10 is wrong with it and why are we not emulating it more?

11 Admiral Rogers: So, first, let us look at what the UK  
12 model is. They basically -- I am going to paint a  
13 simplistic picture. They turned to their intelligence  
14 structure, in this case, GCHQ, which NSA's equivalent. They  
15 turned to GCHQ and said you have the preponderance of  
16 capability, insight, expertise. We would like you to take a  
17 portion of that capability, and we are going to create this  
18 National Cyber Security Centre. In fact, the individual who  
19 runs it, a guy I have worked with for a long time, is a GCHQ  
20 employee. They decided that in their construct they were  
21 comfortable with that.

22 For us on the U.S. side, we have always been less  
23 comfortable with the idea of, well, do you want the  
24 intelligence world to be the primary interface, if you will,  
25 with the private sector. For our UK teammates, they are

1 just very comfortable with that. And their view is it is  
2 about aligning the greatest expertise and capability with  
3 the private sector, and there is not quite the same baggage  
4 or at least history or tradition.

5       Because of that, on the U.S. side, we have taken a very  
6 fundamental different approach, I am hoping with this new  
7 team coming in, this is opportunity for us to step back and  
8 say to ourselves are we happy with the way this is working.  
9 I have not seen your diagram, but you have heard me say for  
10 a long time we have got to simplify the complexity of this  
11 structure to the outside world because if you are in the  
12 private sector and you are trying to figure out so who am I  
13 supposed to be dealing with and why this time was it you and  
14 the last time it was that organization and the next time you  
15 are telling me you want me to go there. We have got to  
16 simplify this.

17       Senator McCaskill: Well, I am down for that. And I  
18 think the curse and the blessing is how protective we are of  
19 classified information. And I understand that challenge.  
20 But boy, oh, boy, pulling this group together after a  
21 significant cyber event, there is going to be a lot of  
22 Monday morning quarterbacking over whether or not more  
23 information should have been shared.

24       Admiral Rogers: If I could also make one point. I  
25 agree with everything you said, but I would remind people

1 perfect information sharing in terms of classified in and of  
2 itself will not necessarily fix every problem. If you look  
3 at reactions to the Russian hack, there were plenty of  
4 organizations that were provided the specific insights who  
5 just opted, for a variety of reasons, not to react in the  
6 same way. And that was not about classification. So I just  
7 want to make people -- I just want us to think us to think  
8 about, hey, this is the simple cure-all.

9 Senator McCaskill: I get it.

10 Admiral Rogers: And I am not trying to say that you  
11 are painting that, ma'am.

12 Senator McCaskill: No. I know it is not the simple  
13 cure, but I know that that underlying disease about  
14 information sharing goes deep and it is calcified. And I  
15 want to make sure that we are aware of that.

16 Admiral Rogers: Yes, Senator.

17 Senator McCaskill: Thank you, Admiral.

18 Senator Reed [presiding]: On behalf of Chairman  
19 McCain, Senator Shaheen, please.

20 Senator Shaheen: Thank you, Mr. Chairman.

21 And thank you, Admiral, for being here and for the job  
22 that you do.

23 And just to pick up a little bit on Senator McCaskill  
24 and the issue of classified versus unclassified, the  
25 challenge with, in this case, the Russian hack with so much

1 of the information being classified is that the American  
2 public does not know what is going on. And when the  
3 American public does not know what is going on on an event  
4 of this magnitude, that is a real challenge for our  
5 democracy.

6 And I was not able to hear your testimony and the  
7 questions, obviously, because I was in another hearing. But  
8 I know that there have been a number of questions about the  
9 Russian hacking and what that means. But have you talked  
10 about what in the big picture that means? What is Russia  
11 really trying to do with the hack of our electoral system,  
12 with the hack of France, with the interference in Germany,  
13 with what they have done in many of the Balkan countries, in  
14 Eastern Europe? What is their goal?

15 Admiral Rogers: Well, I am going to talk about the  
16 U.S. side and then talk about it more broadly.

17 So on the U.S. side, as we indicated, speaking to you  
18 now as the Director of NSA, as we said in the intelligence  
19 community assessment, three primary goals we thought.

20 First was to undercut the United States and its broad  
21 principles of democracy and try to send a message, hey,  
22 look, these guys are every bit as inconsistent as everybody  
23 else. They are not this high-on-the-hill, perfectly white  
24 and perfect structure. Look, they have pettiness. They  
25 work against each other. So to undercut our democracy.

1           Secondly, they clearly had a preference that candidate  
2 Clinton not win, and they also wanted to ensure if she did  
3 win, that she was weakened.

4           And then the report talks about the third objective was  
5 to try -- and this is where NSA has a difference confidence  
6 level than my other teammates. But I agree with the  
7 judgment that the third objective was to help candidate  
8 Trump win. If you look at the activity they have done in  
9 the United States, if you look at the activity they have  
10 done in France, in Germany, they clearly are trying to help  
11 ensure that leaders they believe might be more inclined --  
12 it does not mean that they necessarily are, but the Russians  
13 appear to be assessing that some leaders might be more  
14 inclined to be supportive of their positions, their views,  
15 might engage in policies more favorable from a Russian  
16 perspective. You saw that just play out in the French  
17 election where there clearly was a difference between these  
18 two candidates and their views of Russia and the things they  
19 were talking in the campaign about if they won, what would  
20 some of their choices be in terms of national security  
21 policies for France and how that might impact the Russians.

22           Senator Shaheen: But is the overarching strategy not  
23 not so much who the winners and losers are, but it is to  
24 undermine the public confidence in a democracy and how it  
25 works?

1           Admiral Rogers: That is why I say that is a part of  
2 it. I am sorry if I did not make that jump on the foreign  
3 side as well. It is the same thing. That is an aspect of  
4 it.

5           Senator Shaheen: Right. So just as they are engaging  
6 in a military buildup, just as they are engaging in the  
7 cyber intrusions, that the other thing they are engaging in  
8 is an effort to undermine Western democracies. That is  
9 another way they are going to undermine the West.

10          Admiral Rogers: Right, to weaken them, to forestall  
11 their ability to respond because there is no political  
12 consensus because they distrust their institutions as  
13 citizens, et cetera. Yes, ma'am.

14          Senator Shaheen: So I was in Poland after the Munich  
15 Security Conference and met with a number of officials  
16 there. And some of the people that we met with suggested  
17 that they were very concerned that we had not responded to  
18 the Russian attack of our election system. And one of the  
19 things that really impressed me was the person who said, you  
20 know, if you are not willing to do anything about what  
21 Russia did in the United States intervening in your  
22 electoral system, fundamental to your democracy, how should  
23 we have any confidence that you will defend us when the  
24 Russians come after us.

25          So what does it say to our allies that we have not been

1 willing to take any overarching action against Russia for  
2 what they did? We have not been willing to pass stronger  
3 sanctions. We have not been willing to do other efforts to  
4 take action against them because of their interference.  
5 What does that say to our allies?

6 Admiral Rogers: So I can certainly understand why our  
7 allies would be perplexed. If this conduct occurred, why  
8 are we not seeing X, Y, or Z? I certainly can understand  
9 that.

10 One of the things we try to assure our allies, though,  
11 is this is one aspect of a broader set of issues. You  
12 should not question -- it depends on the relationship, but  
13 in broad terms, you should not call into question our long-  
14 term commitment to you, for Poland, for example. Do not let  
15 there be any doubt of that.

16 Senator Shaheen: So we are more committed to Poland  
17 than we are to addressing Russia's --

18 Admiral Rogers: That is not what I said.

19 Senator Shaheen: I know it is not what you said. But  
20 it leaves open to interpretation that assumption. So thank  
21 you.

22 Admiral Rogers: Yes, ma'am.

23 Senator Reed: Thank you.

24 Admiral Rogers, thank you for your testimony today. As  
25 always, we appreciate your service, and would you

1 communicate to your colleagues our appreciation for their  
2 service also?

3 On behalf of Chairman McCain, the hearing is adjourned.

4 [Whereupon, at 11:48 a.m., the hearing was adjourned.]

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25