

Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON UNITED STATES CYBER
COMMAND IN REVIEW OF THE DEFENSE AUTHORIZATION REQUEST
FOR FISCAL YEAR 2017 AND THE FUTURE YEARS DEFENSE PROGRAM

Tuesday, April 5, 2016

Washington, D.C.

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

1 HEARING TO RECEIVE TESTIMONY ON UNITED STATES CYBER COMMAND
2 IN REVIEW OF THE DEFENSE AUTHORIZATION REQUEST FOR FISCAL
3 YEAR 2017 AND THE FUTURE YEARS DEFENSE PROGRAM
4

5 Tuesday, April 5, 2016
6

7 U.S. Senate
8 Committee on Armed Services
9 Washington, D.C.
10

11 The committee met, pursuant to notice, at 9:33 a.m. in
12 Room SH-216, Hart Senate Office Building, Hon. John McCain,
13 chairman of the committee, presiding.

14 Committee Members Present: Senators McCain
15 [presiding], Inhofe, Sessions, Ayotte, Fischer, Cotton,
16 Rounds, Ernst, Tillis, Graham, Reed, Nelson, McCaskill,
17 Manchin, Shaheen, Gillibrand, Blumenthal, Donnelly, Hirono,
18 Kaine, King, and Heinrich.
19
20
21
22
23
24
25

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

3 Chairman McCain: Good morning. Committee meets today
4 to receive testimony from Admiral Mike Rogers, the
5 Commander of U.S. Cyber Command, Director of the National
6 Security Agency, and Chief of the Central Security Service.

7 A lot of titles, Admiral. That's good. Thank you for
8 your many years of distinguished service and for appearing
9 before this committee today.

10 Threats to our national security in cyberspace
11 continue to grow in speed and severity. New attacks appear
12 in the headlines on an increasingly frequent basis as
13 nation-states, criminal organizations, and terrorists seek
14 to leverage technology to steal, coerce, and deter. When
15 you appeared before this committee in September, Admiral
16 Rogers, you noted that we, quote, "have peer competitors in
17 cyberspace" and that some of them have, quote, "already
18 hinted that they hold the power to cripple our
19 infrastructure and set back our standard of living if they
20 choose."

21 Since that hearing, Russia has demonstrated the
22 ability to cut power to hundreds of thousands of people in
23 central and western Ukraine. This attack, the first
24 confirmed successful cyberattack on a large-scale power
25 grid, is terribly significant, as it demonstrates a

1 sophisticated use of cyberweapons as a destabilizing
2 capability and an effective deterrence tool. With Russia,
3 China, and other potential adversaries developing
4 capabilities intended to deter us along with our friends
5 and allies, we must develop not only an effective
6 deterrence policy, but also the capabilities necessary to
7 deter any nation seeking to exploit or coerce the United
8 States through cyberspace.

9 After significant urging by this committee, I believe
10 the Defense Department is -- recognized this need, and
11 important progress has been made at Cyber Command. But,
12 there's still a lot of work to do. For the most part, the
13 services appear to be on track to meet the goal for the
14 development of a 6,200-person cyberforce, but unless we see
15 dramatic changes in future budgets, I'm concerned that
16 these well-trained forces will lack the tools required to
17 protect, deter, and respond to malicious cyberbehavior. In
18 short, unless the services begin to prioritize and deliver
19 the cyberweapon systems necessary to fight in cyberspace,
20 we're headed down the path to a hollow cyberforce. Just as
21 it would be unacceptable to send a soldier to battle
22 without a rifle, it's unacceptable to deprive our
23 cyberforces the basic tools they need to execute their
24 missions. Some service budgets omitted funding for even
25 the most basic tools, like those necessary for

1 cyberprotection teams to assess and triage compromised
2 networks. This is unacceptable, and I look forward to
3 hearing your assessment, Admiral Rogers, of the military
4 service's commitment to equipping the cyberforce. I also
5 look forward to hearing whether the new acquisition
6 authorities we provided Cyber Command in the Fiscal 2016
7 NDAA will help address some of these service-induced
8 shortfalls.

9 While I'm encouraged by some of the progress of the
10 Department of Defense in Cyber Command, I remain concerned
11 that the administration's cyberpolicy, as a whole, remains
12 detached from reality. For years, our enemies have been
13 setting the norms of behavior in cyberspace while the White
14 House sat idly by, hoping the problem will fix itself. In
15 December, the administration provided its response, nearly
16 a year and a half late, to this committee's requirement for
17 a cyberdeterrence policy. The response reflected a
18 troubling lack of seriousness and focus, as it simply
19 reiterated many of the same pronouncements from years past
20 that have failed to provide any deterrent value or decrease
21 the vulnerability of our Nation in cyberspace. I applaud
22 the recent efforts of the Justice Department to name and
23 shame Iran for its cyberattacks against our critical
24 infrastructure and financial sector. But, again, I remain
25 puzzled as why it took nearly 5 years after Iran began

1 attacking U.S. banks for the administration to begin doing
2 so. That kind of indecisiveness is antithetical to
3 deterrence, and our Nation simply cannot afford it.

4 Let me close by thanking you, Admiral Rogers, for your
5 leadership at Cyber Command. You've always been very
6 candid and forthcoming before this committee, and we
7 appreciate that very much. We're finally beginning to
8 field the cybercapabilities we need for the future. As we
9 confront the challenges ahead, this committee remains
10 committed to doing everything we can to provide you and the
11 men and women you lead with the tools necessary to defend
12 our Nation in cyberspace. I look forward to your
13 testimony.

14 Senator Reed.

15
16
17
18
19
20
21
22
23
24
25

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

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

4 I, too, would like to welcome Admiral Rogers back to
5 the committee -- thank you, sir -- and to express my
6 gratitude to you and -- but also to the men and women that
7 you lead, the military and civilians who work to secure the
8 department of networks, support the combatant commands in
9 cyberspace, and defend the Nation against major
10 cyberattacks.

11 Cyber Command is at another set of crossroads. The
12 committee received testimony last fall from multiple
13 witnesses recommending elevation of Cyber Command to a full
14 unified command. I understand that elevation has been
15 discussed by the Joint Chiefs, and that the Secretary is
16 considering this recommendation as part of the Goldwater-
17 Nichols reform effort. I would like to hear, Admiral, in
18 your testimony and your comments, your views on the
19 readiness of the Command for elevation and on the related
20 issue of sustaining the dual-hat arrangement under which
21 the Commander of Cyber Command also serves as the Director
22 of the National Security Agency.

23 Six years after Cyber Command was established, the
24 military services are just now presenting trained military
25 cyberunits to command. A little more than half of the

1 planned units have reached initial operational capability.
2 This is a major milestone, but trained individuals are only
3 one part of military readiness. The other pieces are unit-
4 level training and proficiency and equipping the forces.
5 The Defense Department is only at the beginning phase of
6 building a unit-level training environment. There are
7 shortages and capability shortfalls in the toolkits
8 available for the Cyber Protection Teams, and the
9 Department has not yet developed a plan for or selected a
10 service executive agent to acquire foundational situational
11 awareness and command-and-control systems for our
12 cyberforces. I look forward to a status report from you,
13 sir, about the pace of progress in these areas.

14 There are other foundational challenges. The
15 Department has deployed, and is in the process of
16 acquiring, additional capable cybersecurity centers at all
17 layers of its networks, from the large perimeter gateways
18 to the millions of individual computers spread across the
19 globe. Cyber Command has dozens of Cyber Protection Teams
20 assigned to defend key segments of our networks, while the
21 military services and the Defense Information Systems
22 Agency have their own computer network defense
23 organizations. A major task now is to integrate these
24 centers and organizations under joint operational concepts
25 to enable real teamwork. And, Admiral, again, I will be

1 interested in your thoughts on this very difficult issue.

2 I am pleased that Cyber Command is joining the
3 initiative to leverage the innovation of the commercial
4 informational technology industry for both cybersecurity
5 and its other missions. To keep pace with a rapidly
6 changing threat, it makes sense to partner with an industry
7 that innovates at the same pace. And, Admiral, I'm
8 interested in hearing how you plan to apply the acquisition
9 authorities the committee granted to Cyber Command in last
10 year's Defense Authorization Act to working with the
11 information technology sector, in particular.

12 Finally, Mr. Chairman, I would note that Admiral
13 Rogers, in his prepared statement for the hearing today,
14 quoted the Director of National Intelligence to the effect
15 that China is still engaged in economic theft in cyberspace
16 and that, quote, "Whether China's commitment of last
17 September moderates its economic espionage remains to be
18 seen." It is obviously a very serious matter if China does
19 not live up to President Xi's pledge to President Obama.
20 And again, I would be interested in your comments, sir, on
21 this issue.

22 Thank you for your service. And I look forward to
23 your testimony.

24 Chairman McCain: Admiral Rogers, welcome back.

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. Good to be back.

5 Chairman McCain, Ranking Member Reed, and
6 distinguished members of the committee, I am pleased to
7 appear before you today to discuss the opportunities and
8 challenges facing U.S. Cyber Command. And I'd like to
9 thank you for convening this forum.

10 It's an honor to represent the individuals of this
11 fine organization, and I'm grateful for, and humbled by,
12 the opportunity to lead this impressive team. I'm
13 confident you'd be extremely proud of the men and women of
14 U.S. Cyber Command if you saw their commitment to mission
15 and hard-earned successes on a daily basis, as I am
16 fortunate to do.

17 While my written statement goes into greater detail,
18 I'd like to briefly highlight the challenges we face in
19 today's environment and also some of the initiatives that
20 the Command is pursuing to meet those challenges.

21 Over the last year, we've seen an increase of
22 cyberspace operations by state and nonstate actors. We've
23 seen a wide range of malicious cyberactivities aimed
24 against both government and private-sector targets. At
25 U.S. Cyber Command, we focus on actors that pose a threat

1 to our national interests through cyberspace. Nations
2 still represent the gravest threats to our Nation's
3 cybersecurity, but we continue to watch closely for signs
4 of nonstate actors making significant improvements in their
5 cybercapabilities.

6 Malicious actors use cyberspace to steal intellectual
7 property and citizens' personal information; and criminals'
8 increasing use of ransomware to extort companies is a
9 worrisome trend. Malicious actors have also intruded into
10 networks, ranking from the Joint Staff's unclassified
11 network to networks controlling our Nation's critical
12 infrastructure. These threat actors are using cyberspace,
13 I believe, to shape potential future operations, with a
14 view to limiting our options in the event of a crisis.
15 Despite this challenging environment, U.S. Cyber Command
16 continues to make progress as it emphasizes shifts to
17 operationally -- operationalizing the Command and
18 sustaining its capabilities.

19 Over the past year, we've continued building the
20 capability and capacity of Cyber Command while operating at
21 an increased tempo. We continue to make progress in
22 building the cyber mission force of the 133 teams that will
23 be built and fully operational by 30 September 2018.
24 Today, we have 27 teams that are fully operational and 68
25 that have attained initial operational capability. And

1 it's important to note that even teams that are not fully
2 operational are contributing to our cyberspace efforts,
3 with nearly 100 teams conducting cyberspace operations
4 today. For example, the Command continues to support U.S.
5 Central Command's ongoing efforts to degrade, dismantle,
6 and ultimately defeat ISIL. Last year, we noted we had
7 just established the Joint Force Headquarters DOD
8 Information Networks. Today, I can probably report the
9 JFHQ DoDIN, as we call it, has made great strides towards
10 its goal of leading the day-to-day security and defense of
11 the Department's data and networks. Also, as the DOD
12 expands the joint information environment, we will have
13 significantly more confidence in the overall security and
14 resilience of our systems. Our operations to defend DOD
15 networks and the Nation's critical infrastructure proceed
16 in conjunction with a host of Federal, industry, and
17 international partners.

18 Recognizing that DOD is just one component of the
19 whole-of-nation's cyber team, U.S. Cyber Command's own
20 annual exercises, CYBERFLAG and CYBERGUARD, offer unmatched
21 realism as we train with Federal, State, industry, and
22 international partners. Additionally, Cyber Mission Teams
23 and Joint Cyber Headquarters are regular participants in
24 the annual exercises of all the combatant commands. While
25 our training is improving, we need a persistent training

1 environment, which the Department is continuing to develop,
2 to gain necessary operational skills and to sustain
3 readiness across our force.

4 I'm excited by the innovation, cultural shift, and
5 focus on long-term strategy that is emerging in the Command
6 and the DOD. In the last year, we've established a Point
7 of Partnership Program in Silicon Valley to link Command
8 personnel to some of the most innovative minds working in
9 cyberspace. Our program is aligned and colocated with the
10 Department's Defense Innovation Unit Experimental, or DIUX,
11 and we are building on the synergy among all DOD elements
12 under the DIUX umbrella.

13 Last September, the Department identified the need to
14 transform DOD's cybersecurity culture by improving
15 individual performance and accountability. The Secretary
16 and Chairman approved the DOD Cyber Security Culture and
17 Compliance Initiative to address those concerns. Cyber
18 Command was identified as the mission lead for this
19 initiative, and is working closely with the Joint Staff and
20 OSD to build the requisite capacity and structure. Cyber
21 Command is also actively contributing to the implementation
22 of the new DOD cyber strategy. The strategy, released in
23 April of 2015, provides a detailed plan to guide the
24 development of DOD's cyberforces and strengthen DOD's
25 cyberdefense and cyberdeterrence posture. The pervasive

1 nature of cyberspace throughout all facets of life and
2 across geographic boundaries, coupled with a growing
3 cyberthreat, makes deterrence in cyberspace a challenge,
4 but evermore important. A proactive strategy is required
5 that offers deterrent options to the President and
6 Secretary of Defense, to include integrated cyberspace
7 operations to deter adversaries from action and to control
8 escalation.

9 To help with all of this, we requested and received
10 enhanced acquisition and manpower authorities. And I thank
11 Congress and the President for the authorizations granted
12 to Cyber Command in the Fiscal Year '16 NDAA. This
13 represents a significant augmentation of our ability to
14 provide capabilities to our Cyber Mission Teams as well as
15 our ability to attract and retain a skilled cyber
16 workforce. We are currently studying how to best implement
17 those provisions, and laying the groundwork needed to put
18 them into effect while, in parallel, evolving a formalized
19 synchronization framework to optimize the employment of our
20 Cyber Mission Force.

21 With that, thank you again, Mr. Chairman and members
22 of the committee, for convening this forum and inviting me
23 to speak.

24 [The prepared statement of Admiral Rogers follows:]

25

1 Chairman McCain: Well, thank you, Admiral Rogers.

2 General Dempsey was asked about our ability to address
3 challenges to this country, and he basically -- he stated
4 that we have significant advantages in every major
5 challenge, except one, and that was cyber. Do you agree
6 with General Dempsey's comment, about a year ago?

7 Admiral Rogers: I do. The phrase I use internally
8 with him is, "Cyber is one area we have to acknowledge that
9 we have peer competitors who have every bit as much
10 capacity and capability as we do."

11 Chairman McCain: That, I would say to my fellow
12 members of the committee, emphasizes our need to address
13 this issue in a comprehensive fashion. So, after we finish
14 the defense bill, I would -- I will spend a great deal --
15 this committee will spend a great deal of its time on this
16 issue, since the threat is as Admiral Rogers just stated.

17 You stated, last year in a House hearing, there's
18 still uncertainty about how we would characterize what is
19 offensive and what is authorized. Again, that boils down,
20 ultimately, to a policy decision. And to date, we have
21 tended to do that on a case-by-case basis. In other words,
22 do we preempt? Do -- if we respond, how do we respond?
23 All of those, it seems to me, are policy decisions that
24 have not been made. Is that correct?

25 Admiral Rogers: I guess, Chairman, the way I would

1 describe it is, we clearly still are focused more on an
2 event-by-event particular circumstance. And I think, in
3 the longrun, where clearly I think we all want to try to
4 get to is something much more broadly defined and well
5 understood.

6 Chairman McCain: So that you understand, when you
7 detect a -- an attack or as to exact -- or detect a
8 probable attack -- I'm -- so, right now, you are acting on
9 a case-by-case basis.

10 Admiral Rogers: Sir.

11 Chairman McCain: Does Russia have the capability to
12 inflict serious harm to our critical infrastructure?

13 Admiral Rogers: Yes.

14 Chairman McCain: Does China have the same capability?

15 Admiral Rogers: Some measure of the same capability,
16 yes.

17 Chairman McCain: How has China's behavior evolved
18 since the OPM breach?

19 Admiral Rogers: We continue to see them engage in
20 activity directed against U.S. companies. The questions I
21 think that we still need to ask is, Is that activity then,
22 in turn, shared with the Chinese private industry? We
23 certainly acknowledge that states engage in the use of
24 cyber as a tool to gain access and knowledge. The question
25 or issue we've always had with the Chinese is, what --

1 while we understand we do that for nations to generate
2 insight, using that then to generate economic advantage is
3 not something that's acceptable to the U.S.

4 Chairman McCain: Do you agree that the lack of
5 deterrence or repercussions for malicious cyberbehavior
6 emboldens those seeking to exploit the U.S. through cyber?

7 Admiral Rogers: Yes.

8 Chairman McCain: Admiral, we are looking carefully at
9 a consolidation of command, here, as far as your
10 responsibilities are concerned. I believe that the
11 Secretary of Defense will also support such a move, so I
12 will be recommending to the committee that we include that
13 consolidation in the defense authorization bill as we mark
14 up. I think my friend Senator Reed also agrees with that.

15 Would you agree that probably the issue of
16 cyberwarfare is the least understood by all of our
17 leadership, including in government, executive and
18 legislative branch?

19 Admiral Rogers: It's a -- it's certainly among the
20 least understood. I think that's a fair --

21 Chairman McCain: And is part of this problem is that
22 this challenge is rapidly evolving?

23 Admiral Rogers: I think that's -- that's clearly an
24 aspect of it, the speed and the rate of change, as well as
25 the complexity. It can be intimidating. I'd be the first

1 to acknowledge that many people find this a very
2 intimidating mission area.

3 Chairman McCain: If you had a recommendation for this
4 committee and Congress as to your significant two or three
5 priorities, what would you recommend?

6 Admiral Rogers: In terms of --

7 Chairman McCain: Of action --

8 Admiral Rogers: -- cyber, overall?

9 Chairman McCain: -- action that you'd like to see the
10 Congress and the executive branch take.

11 Admiral Rogers: I think we clearly need a focus on
12 ensuring, number one, that we've got our defensive house in
13 order and that we're able to defend our systems as well as
14 our networks. And we need to think beyond just networks,
15 into our individual --

16 Chairman McCain: Which --

17 Admiral Rogers: -- combat and weapon --

18 Chairman McCain: -- which, to me, means a policy, but
19 please go ahead.

20 Admiral Rogers: Secondly, we need to continue to
21 generate the complete spectrum of capabilities to provide
22 options for our policymakers, as well as our operational
23 commanders, so, when we have these issues, we've got a
24 series of capabilities that we can say, "Here are some
25 capabilities that we can choose from."

1 And then, lastly, I think we've just got to -- the
2 other point I'd try to make is, we've got to figure out how
3 to bridge across not just the DOD, but the entire U.S.
4 Government, with the private sector about how we're going
5 to look at this problem set in an integrated national way.

6 Chairman McCain: Would you also agree that
7 sequestration could threaten you with a hollow force after
8 you have recruited and -- some of the brightest minds in
9 America to help you?

10 Admiral Rogers: Oh, very much so. I would highlight,
11 in FY13, when we shut down the government, I can remember
12 going -- I was in a different job at the time, but still I
13 was doing -- leading the Navy's cyber effort. And as much
14 of my workforce said, "So, explain to me, Admiral, why we
15 should stay with you, if this is what we're going to have
16 to deal with on an aperiodic basis, being told we're going
17 to be furloughed, we're not going to get paid." I can
18 remember telling them, in '13, "Please stay with us. This
19 -- I hope this is a one-time thing."

20 Chairman McCain: But, sequestration means further
21 hampering of --

22 Admiral Rogers: It means further -- because
23 everything is -- our ability to meet the timelines that
24 we've been given have been predicated on the sustaining of
25 the budgets. If we go to sequestered levels, I will not be

1 capable of generating that capability in a timely way that
2 right now we're on the hook to do.

3 Chairman McCain: Senator Reed.

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

5 And one of the issues that has been discussed, and I
6 mentioned in my opening statement, is raising Cyber Command
7 to a full unified command. And yet, I also noted, and you
8 acknowledged, that only half of Cyber Command's uniformed
9 cyber mission forces are initially capable -- IOP -- IOC, I
10 should say. And then, some critical elements, such as
11 persistent training environment, a uniform platform doesn't
12 exist. Are you, in your mind, mature enough to be a full
13 unified command now? Or --

14 Admiral Rogers: Yes.

15 Senator Reed: And what would that advantage give you?
16 Or what would that decision give you?

17 Admiral Rogers: So, generally when we think about
18 what tends to drive should something be elevated to a
19 combatant command -- broadly across the Department, we tend
20 to focus on the imperatives of unity of command, unity of
21 effort, and is it either -- in this case, it would be a
22 functional, not geographic --

23 Senator Reed: Right.

24 Admiral Rogers: -- and, in this case, does the
25 function rise to a global level, and is it of sufficient

1 priority to merit coordination across the entire
2 Department?

3 The other issue, I would argue, is one of speed. All
4 of those argue -- and again, I'm -- I just am one input. I
5 realize this is a much broader decision than just Admiral
6 Rogers, and there's many opinions that will be factored in.
7 My input to the process has been, the combatant commander
8 designation would allow us to be faster, which would
9 generate better mission outcomes. I would also argue that
10 the Department's processes of budget, prioritization,
11 strategy, policy, are all generally structured to enable
12 direct combatant commander input into those processes.
13 That's what they're optimized for. And I believe that
14 cyber needs to be a part of that direct process.

15 Senator Reed: The other aspect, obviously, is the
16 relationship with NSA. And there are several options. One
17 is to have separate commanders, one is to have one
18 commander with a dual hat. Or one option, or additional
19 option, is to, at least at a future time, have the option
20 to divide the dual-hat arrangement. Can you comment on
21 that issue?

22 Admiral Rogers: So, my recommendation has been, for
23 right now, you need to leave them dual-hatted. Part of
24 that is the very premise that we built Cyber Command, when
25 we created it 6 years ago, where we said to ourselves, "We

1 are going to maximize the investments that the Nation had
2 already made in NSA, in terms of infrastructure and
3 capability." So, because of that, we didn't have a huge
4 military construction program, for example, for Cyber
5 Command, and put these cyber mission forces, the 6200, in
6 different structures. We said we were going to take NSA's
7 existing space as a vehicle to do that. So, my input has
8 been, for right now, based on the very model we created
9 Cyber Command, where we really, in many ways, very tightly
10 aligned these two organizations, that, at the current time,
11 it would be difficult -- not impossible -- first to
12 acknowledge that -- it would be difficult or less than
13 optimal, in my opinion, to try to separate them now. But,
14 what I have also argued is, but we need to continue to
15 assess that decision over time. And you need to make it a
16 conditions-based assessment as to, At some point in the
17 future, does it make more sense to do that?

18 Senator Reed: And part of that is the fact that if
19 you are a unified command, you will be developing
20 alternatives to NSA capabilities --

21 Admiral Rogers: Yes.

22 Senator Reed: -- exclusive to Cyber Command, so that,
23 at some point, you could have an infrastructure that looks
24 remarkably like NSA, and these synergies you're talking
25 about now aren't operational --

1 Admiral Rogers: As important, right. Yes, sir.

2 Senator Reed: One of the issues is that, as a -- you
3 depend upon the services to provide you a great deal of
4 resources. In fact, it is really, I think, interesting to
5 note that only half of these identified units are, at least
6 initially, capable, and that there's -- doesn't seem to be
7 an intense training effort that's standardized and in place
8 right now. What can you do -- what can we do to accelerate
9 these units, in terms of their maturity and their training
10 environment?

11 Admiral Rogers: So, if I could, Senator, I'm going to
12 respectfully disagree.

13 Senator Reed: That's quite all right. You don't even
14 -- well, you have to be respectful.

15 [Laughter.]

16 Admiral Rogers: Remember, we started this build
17 process in fiscal year '13. And we said that we would
18 finish it by the end of fiscal year '18, full capability
19 and ready to fight in a high- --

20 Senator Reed: Right.

21 Admiral Rogers: -- -demand environment. We're pretty
22 much on track, as I have said publicly. If you look right
23 now -- in fact, in the last 2 months, I've actually managed
24 to increase timeliness since the last assessment I did in
25 February, where I publicly had said, based on the data as

1 of the 1st of February, I believe that we'll meet IOC for
2 91 percent of the teams on time, and that we will meet FOC
3 for 93 percent of the teams on time. In the 2 months since
4 then, we're up -- I managed to work with the services, and,
5 for IOC, we're up to about 95 percent of the force; and,
6 for FOC, we're at about 93 -- we're still at 93 percent of
7 the force. So, my only point is, I'm not critical of the
8 services, in terms of their generating the force. I think
9 they're making a very good effort, and it's on track. It's
10 not perfect, but it's not -- on track.

11 They've also been very willing -- when I've said,
12 "What we need to do is ensure that we have one integrated
13 joint category to how we work cyber," so there's got to be
14 one structure, one training standard -- every service has
15 agreed to adhere to that. So, in that regard, I'm also
16 very comfortable what the services are doing.

17 What I think the challenge for us as I look over the
18 next few years is, we initially focused on those mission
19 teams and the men and women and their training. What
20 experience is teaching is -- not unlike other domains, is
21 -- and as you both, the Chair and Ranking Member, said in
22 your opening statements, that's not enough. And so, what
23 we're fighting now is, it's the other things that really
24 help enable -- we've got to focus more on.

25 Senator Reed: Thank you.

1 Thank you, Mr. Chairman.

2 Chairman McCain: Senator Inhofe.

3 Senator Inhofe: Thank you, Mr. Chairman.

4 Admiral Rogers, in December of last year, you
5 published an article saying, "A challenge for the military
6 cyber workforce," and you discussed, as you did in your
7 written statement today, that -- the importance of growing
8 and developing and maintaining this force. When you talked
9 about -- well, I guess it was the Chairman, in his
10 statement -- the 123 teams, where you are right now, and
11 aiming to 133, what comprises a cyber team?

12 Admiral Rogers: They come in several different types.
13 There is what we call Combatant Command Mission Teams.
14 Those are aligned with combatant commanders. They are
15 generally designed to create offensive capability, if you
16 were -- will.

17 Senator Inhofe: Yeah.

18 Admiral Rogers: There are Cyber Protection -- those
19 are about -- and that team, CCMTs, Combatant Commander
20 Mission Teams --

21 Senator Inhofe: Yeah.

22 Admiral Rogers: -- there are about 65 individuals on
23 a team. If you look at Cyber Protection Teams, slightly
24 different mission, so different structure, different focus
25 -- they're at about 39 individuals per team. Each of those

1 two teams, the Combatant Commander Mission Team, the Cyber
2 Protection Team --

3 Senator Inhofe: Okay.

4 Admiral Rogers: -- has a small subset of about 23
5 individuals, what we call Support Teams.

6 Senator Inhofe: Well --

7 Admiral Rogers: So, that just gives you a sense for
8 the --

9 Senator Inhofe: Sure.

10 Admiral Rogers: -- range; anywhere from --

11 Senator Inhofe: Sure.

12 Admiral Rogers: -- 20 to 60 --

13 Senator Inhofe: And that's -- when you add all that
14 together, that's when you come up with the 6,187.

15 Admiral Rogers: Yes, sir.

16 Senator Inhofe: And as was brought out in the
17 Chairman's statement, you really have to know -- well,
18 first of all, you're drawing from institutions that are
19 training these people. This is new. This is --

20 Admiral Rogers: Right.

21 Senator Inhofe: This is brand new to a lot of people,
22 including a lot of people at this table. I know that, in
23 my State of Oklahoma, the University of Tulsa has really
24 made great progress. In fact, your predecessor was out
25 there and working with them. And I understand, from

1 Senator Rounds, that a similar thing is happening in South
2 Dakota. So, you've got these kids out there, they're
3 learning this, they're choosing -- they're determining what
4 they're going to do for a career.

5 Now, I think it's a good question when you say -- when
6 we ask the question, "Can we really depend on sustaining,
7 in this environment that we're in right now, this -- these
8 teams -- this number or this workforce, so that individuals
9 out there will -- would be aiming their talents toward
10 helping us in your" -- because there's going to be a lot of
11 competition for these kids. How confident are you that
12 we're going to be able to maintain the level necessary to
13 attract good people?

14 Admiral Rogers: So, experience to date says we're
15 doing a good job in that regard, both for our ability to
16 recruit and retain. What tends to drive that to date, our
17 experience suggests, is the desire of men and women,
18 whether they're civilian or in uniform, to be part of
19 something bigger than themselves, to do something that
20 matters, and to do something on a cutting edge. That, if
21 you will, is really what powers the men and women of the
22 teams.

23 Senator Inhofe: Yeah.

24 Admiral Rogers: I'm always talking to the -- my
25 fellow leaders about, "So, what are the advance indicators

1 that we should be looking at that would tell us if that
2 trend is changing?" There are a couple skillsets within
3 the mission force, that I've mentioned separately
4 previously, that I may, in fact, come back to the committee
5 with to say, "Look, there may be some additional measures
6 here -- flexibility to hire" --

7 Senator Inhofe: That would be a good thing to do for
8 the record, to come back, because I'm running out of time
9 here, and I'd --

10 Admiral Rogers: Sir.

11 Senator Inhofe: -- a couple of other things I wanted
12 to get to. I agree with you, when you say that the states
13 that we watch most closely in cyberspace remain Russia,
14 China, Iran, and North Korea. At the same time, I notice
15 that the -- there is an effort -- and this came when our
16 FBI Director, James Comey, was in contact with these people
17 -- that they've -- they were -- China is trying to develop
18 a closer relationship with us, when, in fact, they're the
19 ones that we're going to be watching. You're not
20 entertaining any kind of a close relationship with them
21 that might impair that --

22 Admiral Rogers: No, sir.

23 Senator Inhofe: -- area. Okay, good.

24 Yesterday, in the -- an article came out on the GAO
25 report that says the Pentagon doesn't know who's in charge

1 for responding to a massive cyberattack. And they go on to
2 talk about the Northern Command. They talk about what we
3 are doing. They're talking about Homeland Security. And
4 you're familiar with this report that came out yesterday?

5 Admiral Rogers: No, I'm not.

6 Senator Inhofe: Oh.

7 Admiral Rogers: But, I'm familiar with the broad
8 premise.

9 Senator Inhofe: Well, okay. Well, the conclusion of
10 the report -- and I'll just read this, and -- it says, "We
11 believe that, by issuing or updating guidance that
12 clarifies roles and responsibilities of relevant DOD
13 officials, DOD will be in a better position to plan for and
14 support civil authorities in a cyberincident." This is a
15 GAO report, so I -- I'd suggest that you look at that and
16 see if we have reached that -- their conclusion so far.

17 Admiral Rogers: Sir.

18 Senator Inhofe: Thank you, Mr. Chairman.

19 Chairman McCain: Senator Manchin.

20 Senator Manchin: Thank you, Mr. Chairman.

21 And thank you, Admiral, for being here and for the
22 work you do. I appreciate it very much.

23 We face a wide range of cyberthreats from terrorist
24 groups, like the ISIS criminal hackers and spies and all
25 the underlying. In nearly every briefing about our

1 national security, I've asked about the issues of
2 cybersecurity and protecting our power grids. And it's a
3 very important issue to me and the amount of power that our
4 little State produces for this country. In the short term,
5 which cyberthreat is most dangerous to the United States?
6 I guess it may -- our grid, our food supply, our water
7 supply? What is most vulnerable that we should be working
8 on?

9 Admiral Rogers: Power and basic infrastructure,
10 something that always concerns me, because the potential
11 impact on the Nation is very significant, should we have
12 significant issues there. I'd also argue -- one sector
13 that I worry about a little bit is -- you look at the
14 amount of personally identifiable information that is
15 resident out there in a lot of various -- healthcare is a
16 good example, where the amount of data that we have all
17 provided to the medical world that is available out there
18 on all of us and our families -- that worries me, about,
19 you know -- and that's reflected -- and you look at OPM,
20 you look at the Anthem health insurance, large data
21 concentrations are now increasingly becoming an attractive
22 target. Because of the power of big data analytics,
23 massive amounts of data that, 10 years ago, we would have
24 said to ourselves, "No one could ever really comb through
25 that to generate insights or find anything. It's just too

1 large." You sure don't have those conversations anymore.

2 Senator Manchin: I mean, we talk about cyber, and we
3 keep talking about, basically, our corporate -- you know,
4 corporate hacking, if you will, for proprietary reasons.
5 And then you look at the military hacking that goes on for
6 our defense reasons, but then you look at just the everyday
7 life --

8 Admiral Rogers: Right.

9 Senator Manchin: -- that we've come to expect that
10 could be probably disrupted with quite an alarming --

11 Admiral Rogers: Yes, sir.

12 Senator Manchin: -- alarming concerns.

13 The other thing I'll -- in your testimony, you
14 mentioned that the Guard and Reserve forces are being
15 assigned to all levels of U.S. Cyber Command and the cyber
16 mission forces. Can you elaborate on what the Reserve
17 component -- specifically, the National Guard -- bring to
18 the table for the cyber mission?

19 Admiral Rogers: Well, you're able -- through our
20 Guard and Reserve teammates, you're able to access a set of
21 manpower that potentially is using these same skillsets in
22 their day-to-day work in the private sector. You're able
23 to also access, at times, a very different perspective,
24 which works out very well, which is one reason why, as we
25 were creating this cyber construct for the Department, we

1 were adamant, from the beginning, it needed to be viewed as
2 a total force, that if we were just going to make this an
3 Active-only component, I was not going to optimize the full
4 range of capabilities that are out there. And so, you've
5 seen, in the last 6 months in particular, the Guard and
6 Reserve capability starting to come online and flesh out,
7 as well.

8 Senator Manchin: The thing I'm -- that I'm saying is,
9 I've -- the National Guard in West Virginia, we don't --

10 Admiral Rogers: Right.

11 Senator Manchin: -- have a base, and our Guard is
12 everything to us. And, being a former Governor, I
13 understand the importance of our Guard. But, we've been so
14 active as, basically, in aggressive recruiting, and some of
15 our best and brightest and youngest people are coming into
16 the Guard for all the opportunities, especially
17 educational.

18 Admiral Rogers: Right.

19 Senator Manchin: It's an area where they can
20 designate and pinpoint for you to bring in some of these
21 really sharp young talents that could help us in defending
22 ourself, cyber. I didn't know if you all look at that.

23 Admiral Rogers: Which is -- the Guard is doing now.

24 Senator Manchin: And they're -- and you all are in --
25 okay.

1 Admiral Rogers: Well, Senator Grassley and I spend a
2 lot of time talking about, How do we do this in an
3 integrated way?

4 Senator Manchin: Again -- well, the other thing -- in
5 your testimony, you state that ISIS main cyber effort is
6 focused on propaganda, recruiting, and radicalization of
7 others. Can you elaborate further on this disturbing
8 statement and how have they been successful?

9 Admiral Rogers: They've harnessed the power of the
10 information arena to promulgate their ideology on a global
11 basis, to recruit on a global basis, to generate revenue
12 and to move money, as well as coordinate some level of
13 activity on a large, dispersed basis. The challenge I look
14 for, or that concerns me when I look at the future, is,
15 What happens if the nonstate actor -- ISIL being one
16 example -- starts to view cyber as a weapon system? That
17 would really be a troubling development on --

18 Senator Manchin: In a very simplistic way -- people
19 ask, Why can't we shut down that part of the Internet? Why
20 can't we interrupt ISIS's ability to go on social media and
21 attract? Why are we not able to infiltrate that more?

22 Admiral Rogers: I mean, I would -- the idea that
23 you're just going to shut down the Internet, given its
24 construction and complexity, is just not --

25 Senator Manchin: I've had people ask me --

1 Admiral Rogers: -- right -- going to be realistic.

2 Senator Manchin: -- "Can't you just stop it from that
3 area of the world where all the problems are coming from,
4 whether it be in the Syria or in parts of Iraq or Iran,
5 things that we might have some input and control over?"
6 It's not possible?

7 Admiral Rogers: It's just not that simple. I wish I
8 could say that there's a part of the Internet that is only
9 used by a specific set of users, but there are all sorts --

10 Senator Manchin: I'm just trying to --

11 Admiral Rogers: -- users out there.

12 Senator Manchin: -- find an answer. But, I think --

13 Admiral Rogers: Yes, sir.

14 Senator Manchin: -- that question is asked quite a
15 bit --

16 Admiral Rogers: Not like that.

17 Senator Manchin: -- "Just shut her down, like turning
18 off your telephone." But, it doesn't work that way.

19 Thank you for your service.

20 Admiral Rogers: Sir.

21 Senator Manchin: Any way this committee can help, I'm
22 sure we'll be there for you.

23 Admiral Rogers: Thanks, Senator.

24 Chairman McCain: Senator Sessions.

25 Senator Sessions: Thank you, Mr. Chairman.

1 And, Admiral Rogers --

2 Admiral Rogers: Sir.

3 Senator Sessions: -- thank you for your service.

4 You're, I believe, the right person at a very challenging
5 time, here in the middle of some decisions that have to be
6 made by the United States sooner rather than later.

7 Our Congress passed -- well, Carl Levin was Chairman
8 then -- we passed a requirement that the Defense Department
9 evaluate the vulnerability of our systems and to issue a
10 report to how to defend those. That time passed, but we've
11 issued another legislation last year that said, "The
12 Secretary of Defense shall, in accordance with the plan,
13 complete an evaluation of the cyber vulnerabilities of each
14 major weapon system of the Department of Defense not later
15 than December 31st, 2019." So, we've given an additional
16 date there. But, "Not later than 180 days after the date
17 of this enactment" -- which I believe would be about May
18 this year, "the Department -- the Secretary of Defense
19 shall submit to the congressional defense committees the
20 plan of the Secretary for the evaluation of major weapon
21 systems, including an identification of each system to be
22 evaluated, an estimate of the funding required, and
23 priority among the evaluations." Are you familiar with
24 that? And are we in -- on track to -- is the Defense
25 Department on track to complete that initial report?

1 Admiral Rogers: I am familiar with it. I'm sorry, I
2 am not in the weapon acquisition business, so I'm not the
3 best informed as to the current status. I know the effort
4 is ongoing, because we, U.S. Cyber Command, are part of
5 that broader effort, partnering with AT&L. I -- if I could
6 just take that one for the record, sir. I apologize --

7 Senator Sessions: Well, if you would, because this
8 has been going on some time. So, on a bipartisan basis,
9 Congress recognized, several years ago, that our weapon
10 systems -- it started out for space, missiles, and
11 antimissile systems being evaluated, and then we realized
12 large segments of our defense capability are vulnerable,
13 and we've had a broader report. I believe it is important
14 for the Secretary to complete this on time, if not sooner.
15 And I would hope that you would look at that.

16 Admiral Rogers: Sir.

17 [The information referred to follows:]

18 [COMMITTEE INSERT]

19

20

21

22

23

24

25

1 Senator Sessions: In light of Chairman McCain's
2 questions and Senator Inhofe's questions, I would refer to
3 this GAO report that just came out. And the first line of
4 this article is, quote, "The Pentagon does not have a clear
5 chain of command for responding to massive cyberattack on
6 domestic targets in the United States, according to the
7 Federal Government's principal watchdog, GAO." Does that
8 concern you?

9 Admiral Rogers: First of all, I haven't read the
10 report, sir, so I'm not informed as to its specifics. I
11 mean, I would argue, hey, I'm always concerned about a
12 clear chain of command and a clear articulation of
13 responsibilities.

14 Senator Sessions: Well, it lists a number of things
15 that do appear to be unclear in how we respond. And the
16 Chairman asked you, When do we -- aren't we going to need
17 to develop a policy for how to respond to attacks, and what
18 we might do in response, and how to ratchet up responses
19 relevant --

20 Admiral Rogers: Right.

21 Senator Sessions: -- to the threats that we face?
22 So, I hope that you would look at that.

23 With regard to the worldwide situation, there's
24 commercial and economic and private companies that are a
25 big part of the entire network of cyber worldwide. Many of

1 those impact our allies, our friends. And many of those
2 could -- many companies could be based in countries that
3 are not friendly to us and would like to penetrate our
4 systems. Are you concerned that all of our allies -- Asia,
5 Europe -- need to be aware of this danger? And are we
6 working to make sure that segments of those systems aren't
7 purchased or impacted by entities that could be hostile to
8 our joint interests?

9 Admiral Rogers: So, I share your concern about
10 supply-chain vulnerability, the phrase we use to --

11 Senator Sessions: That's a good --

12 Admiral Rogers: -- describe the --

13 Senator Sessions: -- word.

14 Admiral Rogers: -- to describe that --

15 Senator Sessions: Supply-chain vulnerability, okay.

16 Admiral Rogers: -- is -- and it is growing in
17 probability, if you will, given the nature of the economic
18 world we're living in now. We have a process within the
19 U.S. Government to address these issues from major
20 purchases, companies, national security priorities. We
21 have a specific process in place for some components of DOD
22 infrastructure, like the nuclear world, for example. But,
23 if you look at its proliferation of the issue generally
24 across both our allies and ourselves, this is an issue
25 that's only going to get tougher, not easier.

1 Senator Sessions: Could be going on for decades, it
2 seems to me. And do we need to meet with our allies to
3 develop a unified policy to protect our joint systems?

4 Admiral Rogers: It is a discussion we have with our
5 allies, and it's much -- as you said, this goes across the
6 commercial sector, DOD, government, writ large. It's out
7 there for all of us.

8 Senator Sessions: Well, I thank you for your
9 leadership. There will be a lot of challenges like that in
10 the months --

11 Admiral Rogers: Sir.

12 Senator Sessions: -- to come. And you're at the
13 focal point of a critical issue, and I hope you'll not
14 hesitate to lead and tell us --

15 Admiral Rogers: Sir.

16 Senator Sessions: -- what we need to do to help you.

17 Admiral Rogers: Roger that.

18 Chairman McCain: Senator King.

19 Senator King: Thank you, Mr. Chairman.

20 Admiral Rogers, I need some clarification of what your
21 responsibilities are in Cyber Command. Are you responsible
22 for protecting this country from cyberattacks on private
23 networks and corporations, or is it simply government
24 networks?

25 Admiral Rogers: So, DOD has a responsibility to

1 defend critical infrastructure against events of
2 significant cyber consequence.

3 Senator King: So, critical infrastructure, that --
4 for example, in Maine, in May, we had three urgent-care
5 centers that were hacked. We had Maine General Health,
6 which is one of our major healthcare -- they were hacked.
7 Is that part of your -- what's the definition of "critical
8 infrastructure"?

9 Admiral Rogers: No, there are 16 segments that the
10 Federal Government has identified as having significant
11 implications for the Nation's security. But, the second
12 component, I would argue, of the definition I gave you of
13 the mission is not just the sector that was attacked, so to
14 speak, but also the magnitude of the event. In DOD, we use
15 the phrase "significant cyber consequence." The concern
16 being that the Department of Defense is not resourced, nor
17 is it currently tasked with, defending every single
18 computer structure within the United States. And so, we
19 try to identify, Where can our finite resources be best
20 applied? And so, they're focused on those 16 segments that
21 have been designated as critical to the Nation's
22 infrastructure, and then tripped in those circumstances in
23 which the actions against one of those 16 segments reaches
24 "significant cyber consequence."

25 Senator King: But, in terms of national defense,

1 we're being -- it's death by a thousand cuts. I mean,
2 we're being hacked every day in --

3 Admiral Rogers: Sir.

4 Senator King: -- insurance companies, businesses.
5 Some of it is cyber espionage, as you point out, but some
6 of it is just -- some of it's criminal --

7 Admiral Rogers: Criminal.

8 Senator King: -- but it seems to me we need to be
9 thinking about who is responsible. I mean, I understand
10 you don't call out the Army if there's a criminal in one
11 town. You have local police. But, there's a gap, here.
12 Do you see what I'm saying?

13 Admiral Rogers: Yes, sir.

14 Senator King: There's a gap in our defenses, because
15 we really don't have the infrastructure of the State police
16 or the local police that would protect local interests when
17 they're being attacked. And you have the expertise. There
18 -- we have to work out something as between Cyber Command
19 and local law enforcement, if you will, to protect us from
20 these repeated and continuous and escalating attacks.

21 Admiral Rogers: Although, if I could, I'd urge us to
22 think more broadly than just Cyber Command. I think the
23 challenge is, How do we harness the capacity and capability
24 that is resident within our government structure, teamed
25 with the capabilities that are resident in the private

1 sector? It's much bigger than just --

2 Senator King: Right.

3 Admiral Rogers: -- don't get me wrong, we're
4 definitely a part of this, but I always urge people -- we
5 have got to think much more broadly than --

6 Senator King: Well, I think --

7 Admiral Rogers: -- just the DOD.

8 Senator King: -- that's a good way to articulate it.

9 Don't -- we keep talking, in these hearings. When are
10 we going to have a well-developed and articulated
11 cyberdeterrence strategy? And I emphasize -- in my notes,
12 I underlined the word "articulated." It's not deterrence
13 if it's not articulated. But, we need definition of, What
14 is an act of war? What is a proportional response? What
15 is a mutually-assured-destruction situation? This -- it
16 seems to me that -- is this in the works? And, if so,
17 when?

18 Admiral Rogers: I mean, sir, I don't have a date for
19 you. That's well beyond the mission set of U.S. Cyber
20 Command. I am part of those discussions. I'm the first to
21 acknowledge that. I try to provide an input and just be
22 one voice as to what I think is the direction, broadly,
23 that we need to go. I apologize, Senator, I don't have a
24 specific date or timeline for you.

25 Senator King: But, it just seems to me that, as a

1 matter of policy, that we really need -- this needs to
2 happen. We've been talking about this as long as I've been
3 on this committee, and we aren't there yet. And yet,
4 something terrible is going to happen, and a lot of people
5 are going to say, "Well, why didn't we have a policy? Why
6 don't we have a deterrent policy?"

7 Admiral Rogers: Yes, sir.

8 Senator King: So, I would urge you, with counsels of
9 the administration, to push for a sense of urgency on this
10 question, because if we -- if all we do is defense, and
11 there's no deterrence, ultimately we're going to lose that
12 battle.

13 Admiral Rogers: Yes, sir. It's a losing strategy.

14 Senator King: A final point. And I know that you
15 talked about this earlier. I -- I'm finding it harder and
16 harder to justify your holding two jobs, given the
17 complexity -- I mean, this arrangement was created in 2009,
18 which, in technological terms, is a century ago. And I
19 just can't -- I mean, I understand the relationship between
20 NSA and Cyber Command, but, particularly if we move in the
21 direction, which I think we are, of setting up Cyber
22 Command as its own independent combatant command, to have
23 the same person trying to run those two agencies, I just
24 think is impractical and almost impossible.

25 Admiral Rogers: I've been doing it for 2 years, to

1 date.

2 Senator King: And you've been doing it very well.

3 Admiral Rogers: So, what I -- as I said in my initial
4 comment, I agree that it's something we need to continue to
5 assess. I agree that, in the long run, the, probably, best
6 course of action is to ultimately put both organizations in
7 a position where they're capable of executing their mission
8 in a complementary and aligned way, but in a more separate
9 way. But, the reality is, we're just not ready to do that
10 today, I believe. Now, don't get me wrong. If I am
11 ordered or directed, I get paid to make things happen, and
12 I will execute it to the best of my ability.

13 Senator King: But, I take it you agree that we should
14 move -- Cyber Command should be its own combatant command.

15 Admiral Rogers: I do, sir.

16 Senator King: Yes, sir. Thank you.

17 Thank you, Mr. Chairman.

18 Chairman McCain: Subject to the will of the entire
19 committee, that would be my intention. And I -- Senator
20 Reed and I would propose that on the defense authorization
21 bill. Right, Jack?

22 Senator Reed: I think so, sir. I think that's
23 something we're going to consider. But, I think it's
24 valuable to have Admiral Rogers' comments today and to
25 consider them as we go forward.

1 Chairman McCain: Thank you.

2 Senator Fischer.

3 Senator Fischer: Thank you, Mr. Chairman. I look
4 forward to the discussion on raising Cyber to its own
5 combatant command, and I look forward to our discussions,
6 as a committee, on the importance of cybersecurity for this
7 country.

8 Admiral Rogers, in your prepared statement, you
9 mentioned the cyberattack on Ukraine's power grid, and you
10 also note that you have seen cyberactors for more than one
11 nation exploring the networks of our Nation's critical
12 infrastructure. Do you believe that our national mission
13 teams possess the necessary skills relating to industrial
14 controls and SCADA systems to be able to stop or to recover
15 from an attack on our power grid?

16 Admiral Rogers: We have the skills. The challenge
17 for us, at the moment, is one of capacity. What I mean by
18 that is, in the 2 years I've been in command, I have yet to
19 run into a situation where we didn't have the skillset to
20 apply against the problem. But, the challenge at the
21 moment, because we're still in the midst of that build, is,
22 sometimes that skillset is embodied in an incredibly small
23 number of people. And if we had multiple events
24 simultaneously, for example, that gets to be -- under the
25 -- where we are right now, you snap the chalk today, so to

1 speak, capacity really is the greater concern to me than
2 capability, if you will, if that makes sense.

3 Senator Fischer: Well, I understand your demands on
4 the force to exceed that capacity, but, as you add those
5 capabilities, how are you going to prioritize the duties
6 and the responsibilities that you're going to have? How do
7 you plan to prioritize placing that -- building competency
8 with our industrial control system? Is that going to be
9 something you're going to focus on in the near term, or is
10 it going to take a backseat to maybe some of the other
11 areas that you're looking at for the cyber mission forces?

12 Admiral Rogers: So, it's something we're doing right
13 now. I would also highlight that the very construct of the
14 force, by creating a separate section of the force that is
15 focused purely on defending critical infrastructure -- it
16 was designed to account for that. How do you make sure you
17 prioritize this capability and ensure that at least an
18 element of the force that we are building is focused like a
19 laser on the defend-the-critical-infrastructure mission
20 set? It's a carved-out, separate entity. It's the
21 national mission force, we call it. General Nakasone is
22 the -- my component commander doing that.

23 Senator Fischer: Do you have a plan to work with
24 services, then, on building that --

25 Admiral Rogers: Oh, yes, ma'am.

1 Senator Fischer: Is it near completion? You heard
2 Senator King ask about policy. We've been asking about
3 policy for a long time. We don't have a policy, but -- so,
4 if we don't have a policy, how are we going to develop
5 plans?

6 Admiral Rogers: Well, my -- remind people is -- look,
7 even as we're trying to get to the broader issues that you
8 have all raised, much of which is outside the immediate
9 mission set of Cyber Command, hey, look, our mission is:
10 generate capacity and capability to ensure that we're ready
11 to go as those broader issues are being addressed. So,
12 we're trying to deal with the deterrence piece by
13 generating the capabilities that we think would be part of
14 that deterrence discussion, by generating the defensive
15 capabilities that we think would be part of that deterrent
16 discussion. I don't want to wait for everything to fall in
17 place that -- we just can't afford to do it that way, as
18 perfect as it would be, in some ways. But --

19 Senator Fischer: I agree with you, there -- we don't
20 have time to wait.

21 Admiral Rogers: Yes, ma'am.

22 Senator Fischer: When we look at the Department, what
23 level of communication do you have with different
24 communities within the Department -- say, the -- with
25 regards to acquisition or installations -- to ensure that

1 the items we purchase or the facilities that we're building
2 are able to take those threats that we're looking at from
3 cyber into account?

4 Admiral Rogers: I would tell you the acquisition
5 piece is one of the areas that we still need a lot of work.
6 And it's not because people aren't working hard. But, I've
7 always been struck by the analogy, we would never buy a
8 ship, a tank, an aircraft with the -- without the
9 operational vision driving exactly how we designed it,
10 built it, structured it. And yet, for much of our networks
11 and infrastructure, that has not historically been our
12 model. We just built those. We bought those -- we focused
13 on efficiency and price. We didn't really focus on
14 operational impact, and we really didn't think, at the
15 time, that we'd be dealing with a world in which intruders
16 -- foreign actors, nonstate actors -- would be using those
17 systems as access points to materially degrade our ability
18 to execute our missions as a department. We just didn't
19 anticipate that, decades ago. And that's the world we're
20 in now. We're trying to overcome --

21 Senator Fischer: Well, it's --

22 Admiral Rogers: -- literally --

23 Senator Fischer: -- it's happened in private
24 industry.

25 Admiral Rogers: Right, decades of investment we're

1 trying to overcome.

2 Senator Fischer: And do you -- last question -- do
3 you have any knowledge if our adversaries have targeted any
4 infrastructure on our military bases?

5 Admiral Rogers: Yes.

6 Senator Fischer: Thank you very much.

7 Admiral Rogers: Yes, ma'am.

8 Chairman McCain: Senator Blumenthal.

9 Senator Blumenthal: Thanks, Mr. Chairman.

10 And thank you, Admiral Rogers, for your extraordinary
11 and distinguished service in so many roles over so many
12 years.

13 I want to focus on the challenges of recruiting young
14 people in an age where the best and the brightest who have
15 knowledge in this area have so many opportunities, many of
16 them highly paid and challenging in their professional
17 issues. Young Americans are entering the workforce with
18 computer technology that has been part of their entire
19 lives, not so much for us of a certain age, but for them,
20 yes. And I wonder if you could tell us how successful you
21 and the, obviously, incomparably important forces under
22 your command have been in recruiting and maintaining talent
23 in this time, and what we can do to help.

24 Admiral Rogers: I'm very comfortable with where we
25 are on the uniformed side. The same things that lead a

1 young man or woman in our Nation to decide they want to
2 pick up a rifle and take on that challenge leads men and
3 women to decide they want to put on a uniform and pick up a
4 keyboard. That has not been the biggest challenge. The
5 area that I've told the team we probably need to take a
6 greater look at is on the civilian side of this, because we
7 have got -- our vision is, you've got to create a workforce
8 that is both Active and Reserve military as well as
9 civilian component to it so we get that breadth of
10 expertise that you've referenced.

11 While we're meeting our targets right now on the
12 civilian side, as I've said, there's a couple skillsets
13 already where I think I'm going to have to come back to the
14 committee to say, "Look, I could -- probably need some help
15 here with -- can I come up with some different processes or
16 options that would make things more attractive to,
17 particularly, some very high-end, very small number of
18 skillsets that I don't have huge numbers of, but they're
19 incredibly valuable for us?" That's one area where I'm
20 thinking I'm probably going to have to come back. I have
21 to work this with the Department first, but my experience
22 is telling me, "You know, Mike, we need to step back and
23 take a look at this piece of it."

24 Senator Blumenthal: Is there sufficient -- are there
25 sufficient resources devoted to research, the personnel

1 available to supervise that research, and, in effect,
2 planning for the future?

3 Admiral Rogers: Right. I mean, there's -- I'm not
4 going to pretend for 1 minute that you have all the people
5 and all the money and -- that you would like. It's -- I
6 would argue -- characterize it as reasonable right now.
7 It's not a major issue, in the sense that, as a commander,
8 I've said to myself, "Wow, we've got a significant
9 deficiency here that will impact our ability to execute the
10 missions." I haven't seen that.

11 Senator Blumenthal: I know that you indicated earlier
12 that you haven't read the GAO report.

13 Admiral Rogers: Right. Right.

14 Senator Blumenthal: But, I wonder, focusing on the
15 local capability, and particularly on the private sector,
16 the infrastructure segment that you mentioned earlier in
17 some of your conversations with my colleagues --
18 transportation, financial, electric -- how well are they
19 doing in protecting themselves?

20 Admiral Rogers: I would -- if you look across the 16
21 segments in the private sector that have been designated as
22 critical infrastructure, in terms of impact on the Nation's
23 security, I would argue some are a little -- some are ahead
24 of others. I'd probably put -- financial, for example, not
25 surprising, in the sense that -- has access to more

1 resources than some, has come to the conclusion that cyber
2 potentially calls into question their very business model,
3 since it's built on the idea of trust and the ability to
4 move funds globally simultaneously through these
5 transactions, if you will, that we all believe in and
6 trust. And, on the other hand, there are some industries
7 -- I -- and, in their defense, I look at them, and they're
8 quick to remind me, "Hey, remember, our business model is
9 different. We're a regulated industry." For example, "In
10 order to generate resources to apply to increase our
11 cyberdefense, our cybercapabilities, the only way for us to
12 do that is raise rates. For example, most consumers, not
13 really enthusiastic about that. Most regulatory bodies not
14 necessarily overly enthusiastic about that at the moment."

15 Senator Blumenthal: And those regulated industries
16 would be electricity --

17 Admiral Rogers: Right. Power is an example.

18 Senator Blumenthal: Yeah.

19 Admiral Rogers: There's a couple of others that fall
20 into that.

21 Senator Blumenthal: And are there unregulated
22 industries that are also in need of improvement that you
23 would put at the bottom of that list of readiness?

24 Admiral Rogers: There are some. I've -- think I've
25 publicly previously talked about -- healthcare, for

1 example, is one of the 16 segments I look at, and I --
2 that's an area probably that needs a broader top-to-bottom
3 look, although I'm the first to acknowledge it's really
4 outside my immediate mission area, and I don't bore into it
5 every day. But, as I look at where I'm -- potentially
6 we're going to be tasked to provide our capabilities to
7 partner with, it's an area that I pay attention to.

8 Senator Blumenthal: Thank you very much.

9 Admiral Rogers: Sir.

10 Senator Blumenthal: Thank you, Mr. Chairman.

11 Chairman McCain: Senator Rounds.

12 Senator Rounds: Thank you, Mr. Chairman.

13 Admiral Rogers, first of all, thank you for your
14 service.

15 I find it interesting that, as you work your way
16 through this, you're in a brand new area and you're trying
17 to determine how to respond and how to protect. It seems
18 that when you lay this out -- and you say, like, you have
19 16 different segments within the realm that you're
20 responding to. Fair to say that they break out into either
21 information or data systems and operating systems, in terms
22 of the way that we look at what the data is or the
23 different systems that we're looking at as being vulnerable
24 at --

25 Admiral Rogers: Right.

1 Senator Rounds: -- at a data system being the
2 collection of information on individuals and operating
3 systems being those systems perhaps necessary for the
4 infrastructure within our country? A fair way to break
5 out?

6 Admiral Rogers: I guess that's fair. To be honest,
7 Senator, I've never really thought of it that way. Not
8 that that's a bad way.

9 Senator Rounds: The --

10 Admiral Rogers: I just haven't --

11 Senator Rounds: Well, the reason that I ask is, it
12 would seem that, while information systems would contain
13 material, information that would be of a private nature,
14 perhaps, trade secrets that may very well be information on
15 an individual, such as the information that we lost at the
16 Federal level when our Federal systems were hacked. At the
17 same time, we have an operating system out there for the
18 utilities. We have operating systems out there for dams.
19 We have operating systems for nuclear power plants.
20 Clearly, in those areas, if someone with intent could get
21 into an operating system, they could do significant amount
22 of damage, perhaps bodily injury, as well.

23 Admiral Rogers: Yes.

24 Senator Rounds: Fair to --

25 Admiral Rogers: Yes.

1 Senator Rounds: -- look at it?

2 Based upon that, when you look at your role and the
3 role of Cyber Command, do you see this as protecting -- do
4 you see them different, in terms of how you protect, or do
5 you see your role different with operating systems versus
6 data and information-collection systems?

7 Admiral Rogers: So, our protection scheme, if you
8 will, is based on two different pieces of strategy. The
9 first component of our strategy is -- our intent is to go
10 into foreign space to stop the attack before it ever
11 reaches those systems. The second component of our
12 strategy is to apply defensive capability working directly
13 with each of the individual elements, if you will, to say,
14 "If that fails, we'd also like to work with you on how you
15 might shore up your systems and your vulnerability."

16 The other point I want to make sure I articulate --
17 and I probably should have done a better job this morning
18 -- is, as a reminder, U.S. Cyber Command and DOD, writ
19 large, provide our cyber capabilities in the defense of
20 critical infrastructure in the private sector in
21 partnership and in support of DHS. DHS has overall
22 responsibility in the Federal Government for the provision
23 of government support to the private sector when it comes
24 to cyber. And so, I'd -- I don't want people thinking,
25 "Well, it's just Cyber Command and just the private

1 sector." There's a broader set of players out there that
2 we integrate with and we support as we execute the mission.

3 Senator Rounds: An attack in either case would be
4 done in milliseconds, fair to say? So, unless we have the
5 system in place and we know whether or not we are there to
6 respond or to correct, to protect, in advance, we don't
7 know whether or not we're going to be able to do it in
8 time. At that point, then we simply respond afterwards.
9 Would you say that, today, we have systems in place to
10 appropriately protect -- for lack of a better term, I'm
11 going to call, the operating systems and the information
12 systems that we have -- do you feel that the protocols are
13 there? And I'm going back to what Senator King was --

14 Admiral Rogers: Right.

15 Senator Rounds: -- alluding to earlier. I -- I'm not
16 sure that we have the definitions prepared yet to allow you
17 to respond immediately, within milliseconds, unless we talk
18 about it and we lay it out. Is it there today?

19 Admiral Rogers: So, across the board, with every
20 single component in the private sector, no, it's not.

21 The other point I would make is, cyber is no different
22 than other domains, in the sense that the importance of
23 intelligence to provide us insight as to what is likely to
24 be coming at us gives us the knowledge and insight, the
25 warning, if you will, to anticipate and act in advance.

1 It's every bit as true for the CENTCOM Commander as it is
2 for me in Cyber Command. Warning continues to be critical
3 for both of us.

4 Senator Rounds: Today, if our forces were aware of an
5 attack on them, they have the ability to respond. But, if
6 it was property or entities that are within the United
7 States, do you have the ability to respond today if it is
8 not a military but a civilian or a civil target?

9 Admiral Rogers: So, is there a process? Yes. Is it
10 something that I can do automatically, instantaneously?
11 No.

12 Senator Rounds: Then, it -- in that case, then it
13 would have to happen first, then, because, for all
14 practical purposes, the attack will be instantaneous.

15 Admiral Rogers: Or we have to get the warning in
16 advance, that importance of intelligence. It --

17 Senator Rounds: But, even if you get the warning in
18 advance, in terms of -- it would have to be enough time for
19 you to get out and to have a political discussion, for all
20 practical purposes, about whether or not you can respond --

21 Admiral Rogers: Again, it would depend by the
22 scenario, because there are some elements where we've got
23 mechanisms in place for the application of capability, and
24 it's just a process, if you will, as opposed to a broad --

25 Senator Rounds: But, not one that --

1 Admiral Rogers: -- political decision.

2 Senator Rounds: -- could be done in milliseconds.

3 Admiral Rogers: But -- right, no. I'm not going to
4 pretend for 1 minute that it's something you're going to do
5 in milliseconds.

6 Senator Rounds: Thank you. Thank you, sir.

7 Thank you, Mr. Chairman.

8 Chairman McCain: Senator McCaskill.

9 Senator McCaskill: Thank you, Mr. Chairman.

10 Thank you, Admiral, for being here.

11 Admiral Rogers: Senator.

12 Senator McCaskill: Let me start with your acquisition
13 personnel. Some of the saddest stories of waste have been
14 in the acquisition of IT within the military -- frankly,
15 within government. And a lot of that has had to do with,
16 you know, knowing what you need to buy, when you need to
17 buy it, and when legacy systems need to be scrapped, and
18 how nimble can you be with off-the-shelf -- I'm not sure
19 the military has been a great example of that flexibility
20 and the ability to move with the technology. So, I think
21 these acquisition personnel are pretty important. And so,
22 do you have the ten in place that are supposed -- that we
23 authorized in order for you to make the wisest acquisition
24 decisions possible, in light of a history littered with
25 serious mistakes and lots of -- billions and billions of

1 dollars wasted?

2 Admiral Rogers: Well, first, just a reminder.
3 Remember, Cyber Command, I operate and defend; I don't buy.
4 You have been kind enough -- the committee and the Congress
5 has been kind enough to provide, if you will, an initial
6 capability to do us. We're in the process of hiring those
7 ten individuals that you have authorized. I am very
8 mindful of -- as I remind the team, "It is about generating
9 outcomes, guys. That's why we're granted this authority,
10 and that's what we need to be mindful of. I'm not
11 interested in spending money for the sake of spending
12 money. It's about generating capabilities that directly
13 impact our mission in a material way."

14 Senator McCaskill: Well, I would be interested in how
15 you are acquiring, with more detail, if you --

16 Admiral Rogers: Yes, ma'am.

17 Senator McCaskill: -- would provide it -- how you are
18 finding the right acquisition personnel, and how
19 competitive are we in finding the right acquisition
20 personnel? Because, in many ways, I think that's the key
21 to the kingdom. If we're going to have the capabilities in
22 this space, it -- a lot of it is, you know, people being
23 trained, but a lot of it is also --

24 Admiral Rogers: Oh, yes, ma'am.

25 Senator McCaskill: -- the underlying --

1 Admiral Rogers: You have to buy the right --

2 Senator McCaskill: -- the capabilities.

3 Admiral Rogers: -- capabilities.

4 Senator McCaskill: And so, I just -- I'm really
5 worried about getting the right people --

6 Admiral Rogers: Yes, ma'am.

7 Senator McCaskill: -- making those decisions. So, I
8 would like to stay updated in that progress.

9 [The information referred to follows:]

10 [COMMITTEE INSERT]

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 Senator McCaskill: What kind of coordination is --
2 your command have at this point with our NATO allies, with
3 Israel, with our Arab allies? I'm particularly interested
4 in any coordination and cooperation you have with NGA.

5 Admiral Rogers: So, I'm not going to publicly, in --

6 Senator McCaskill: Obviously.

7 Admiral Rogers: -- unclassified forum, go into the
8 specifics. I would only tell you, we partner with -- we
9 have a handful of nations right now we have a very direct,
10 very real relationship with, with respect to capabilities,
11 real-world operations. I won't go into the specifics of
12 the who.

13 One of the challenges I find is, cyber, like any other
14 mission area, we have got to prioritize. So, when I look
15 at foreign partnerships, I ask, Where is the greatest
16 return for us, as a Department, as the DOD, and where is
17 the greatest return for us, U.S. Cyber Command, in terms of
18 the ability to execute our mission? We've got to -- I
19 spend almost as much time with a discussion with the team
20 about what we're not going to do as what I discuss what we
21 are going to do, because I always remind them, particularly
22 since we're still in the midst of building this capability
23 out, "Prioritization, prioritization, prioritization,
24 guys." We can't do everything. And so, we've identified
25 an initial set of foreign partners, if you will. Those

1 partnerships today are generating capability that we're
2 actually using today.

3 Senator McCaskill: Great. And maybe in a classified
4 setting, I could get more information.

5 Admiral Rogers: Yes, ma'am.

6 Senator McCaskill: What is the ratio of civilian
7 versus military within the Command at this point?

8 Admiral Rogers: It's about -- we're trying to build
9 to about 80 percent military, 20 percent civilian. If you
10 looked at it today as a snapshot, it's probably, off the
11 top of my head, 70/30 -- 70 percent military, 30 percent
12 civilian.

13 Senator McCaskill: And what about contractors? What
14 is the ratio on contractors? And what is your goal on
15 contractors? Because this could be an area -- and, of
16 course --

17 Admiral Rogers: Right.

18 Senator McCaskill: -- you know, underlying that is a
19 concern about the actual screening of contractors. What is
20 your ratio now of contractors to DOD, and what do you want
21 it to be, going forward?

22 Admiral Rogers: We probably, right now -- apologize,
23 I'm trying to do the math in my head -- it's probably about
24 25 percent -- we have an -- over and above the government,
25 civilian, and military -- we have an additional 25 -- off

1 the top of my head, we have about an additional 25 percent
2 in the contractor base.

3 Senator McCaskill: It -- and is that where you would
4 like to be, going forward? Do you see more reliance on
5 contractors, going forward?

6 Admiral Rogers: I'm a little bit leery of over-
7 becoming reliant on contractors. Why? Because I try to
8 remind people, cyber is a domain in which we conduct a wide
9 range of military operations. And, in accordance with the
10 Law of Armed Conflict, those operations need to be
11 conducted by military personnel. So, I'm not trying to
12 minimize the role of contractors. I just try to remind the
13 team, "It's not one-size-fits-all, so we've got to step
14 back and ask ourselves what's the right allocation." I'm
15 pretty comfortable right now. I wouldn't argue that it's
16 among my highest priorities, in terms of increasing the
17 ratio of contractors. I'd argue, right now, probably
18 priority number one, manpower-wise, as I've said, is the
19 civilian piece. I'm very comfortable with -- we're
20 tracking and we're going the right way in the uniformed
21 piece. The civilian area is where I know I'll be paying
22 more attention to in the coming year.

23 Senator McCaskill: Thank you, Admiral.

24 Admiral Rogers: Yes, ma'am.

25 Chairman McCain: Senator Graham.

1 Senator Graham: Thank you for your fine work,
2 Admiral. Can you hear me?

3 Admiral Rogers: Yes, sir.

4 Senator Graham: Okay. What are the threats, nation-
5 state-wise, in terms of who we're most threatened by?

6 Admiral Rogers: I would argue Russia and, again, the
7 -- probably, in terms -- if you look at capability, the
8 other four that we have publicly acknowledged we pay great
9 attention to: China, Iran, North Korea -- and then the
10 nonstate actors, the other category where I look, that
11 could be a game-changer, were the -- some of the dynamics
12 to change.

13 Senator Graham: On the terrorism side, could you give
14 us the top couple of terrorist organizations you're worried
15 about?

16 Admiral Rogers: It's not that I don't know it. In an
17 unclassified forum, I --

18 Senator Graham: Okay, we won't go down that road.

19 Admiral Rogers: If I could. Thank you, sir.

20 Senator Graham: On the criminal side, what areas of
21 criminality do you worry the most about? What countries?

22 Admiral Rogers: I would argue, right now, Russia
23 probably has the most active criminal element, with the
24 most -- with the greatest capability.

25 Senator Graham: Do you think the Russian government's

1 doing anything constructive, in terms of regulating their
2 criminal activity in cyber?

3 Admiral Rogers: I would only say it doesn't appear to
4 be getting much better.

5 Senator Graham: What about Iran? Has Iran gotten
6 better in the last year, in terms of their cyber activity?

7 Admiral Rogers: Yes.

8 Senator Graham: Are they less threatening?

9 Admiral Rogers: I apologize, I'm not sure --

10 Senator Graham: Are they less threatening or just
11 more capable?

12 Admiral Rogers: I'd argue they're increasing their
13 investment, they're increasing their level of capability.
14 We have not seen the same level of activity from them that
15 we have seen historically in the past. I have seen some of
16 that same activity directed at other nations and other
17 groups around the world.

18 Senator Graham: They're improving their capability?

19 Admiral Rogers: Yes, sir.

20 Senator Graham: Do we know if any of the money
21 they're getting from the Iranian nuclear deal is going into
22 their cyber upgrades?

23 Admiral Rogers: I don't know for a fact.

24 Senator Graham: Okay. Is it fair for the country to
25 establish, as a policy, cyber dominance over enemies, that

1 we want to be the -- have a dominance in this area of
2 warfare?

3 Admiral Rogers: I mean, I want to think -- I would
4 argue we want to have the same level of capability in
5 supremacy in cyber as we have articulated that we want in
6 every other --

7 Senator Graham: Okay. Well, that's --

8 Admiral Rogers: -- domain --

9 Senator Graham: I think that's a good goal --

10 Admiral Rogers: -- for our Nation.

11 Senator Graham: -- so let's march down that path.

12 And I associate myself with Senator King about what we need
13 to do as a Nation.

14 Admiral Rogers: Sir.

15 Senator Graham: The Navy. The difference between the
16 Chinese navy, the Russian navy, and the American Navy is
17 pretty wide?

18 Admiral Rogers: Yes, sir.

19 Senator Graham: In the cyber arena, how close is it?

20 Admiral Rogers: I have publicly stated before, the
21 Russians, I would consider in cyber, a peer competitor.
22 China, not in the same place, but rapidly attempting to get
23 there.

24 Senator Graham: So, the gap between the dominance we
25 have on the seas in cyber is not nearly --

1 Admiral Rogers: Not nearly the same.

2 Senator Graham: Okay. When it comes to Iran, when
3 you compare their air force to our Air Force, what's the
4 gap?

5 Admiral Rogers: Oh, significant.

6 Senator Graham: Okay. In the cyber arena, less
7 significant?

8 Admiral Rogers: Less significant, but it's still an
9 area of significant advantage for us, right now.

10 Senator Graham: Are the Iranians trying to close it?

11 Admiral Rogers: Oh, they are.

12 Senator Graham: Okay. So, from a NATO point of view,
13 you're familiar with Article 5, an attack against --

14 Admiral Rogers: Sir.

15 Senator Graham: -- one is an attack against all. Is
16 there any such concept in the cyber arena?

17 Admiral Rogers: You've heard NATO publicly talk about
18 the fact that they believe Article 5 applies to all domains
19 of warfare.

20 Senator Graham: Do they have any rules of engagement
21 that would identify what a cyberattack is?

22 Admiral Rogers: They're probably in the same arena we
23 are: still trying to work our way through that.

24 Senator Graham: When do you think we'll arrive at a
25 conclusion to Senator King's question?

1 Admiral Rogers: Boy, I don't know. The --

2 Senator Graham: What's the biggest impediment to us

3 getting there? Is it the Congress? Is it the --

4 Admiral Rogers: No.

5 Senator Graham: -- DOD?

6 Admiral Rogers: It's as much, in some ways, as -- and

7 again, this is just Mike Rogers' opinion -- it's as much,

8 in some ways, from my perspective, as, "Well, this is just

9 an intellectual exercise. It -- this is something we can

10 afford to" --

11 Senator Graham: The Department --

12 Admiral Rogers: -- "to push down" --

13 Senator Graham: -- of Homeland Security is

14 responsible, basically, for protecting us in the

15 financial/service/power arena, our civilian targets.

16 Admiral Rogers: Sir.

17 Senator Graham: You're responsible for protecting the

18 military infrastructure.

19 Admiral Rogers: And we provide support to that

20 commercial --

21 Senator Graham: That's right.

22 Admiral Rogers: -- infrastructure, if requested.

23 Senator Graham: But, you're also responsible for

24 going on offense. The --

25 Admiral Rogers: Yes, sir.

1 Senator Graham: -- DHS is not going to attack a
2 foreign nation. You would.

3 Admiral Rogers: Yes, sir.

4 Senator Graham: So, how could we, as a Nation, given
5 the threats that we face in the cyber arena, not really
6 have a good answer as to, What's the impediments to
7 creating rules of engagement?

8 Admiral Rogers: I apologize, sir. You really need to
9 speak to the policy side.

10 Senator Graham: Yeah, but you're an operator.

11 Admiral Rogers: Yes, sir.

12 Senator Graham: So, who do you talk to about, "Hey,
13 guys, let's see if we can get there"?

14 Admiral Rogers: So, I'd -- the Secretary of Defense
15 or the Office of the Secretary of Defense.

16 Senator Graham: How do they respond?

17 Admiral Rogers: I think, intellectually, we all
18 realize that that's what we need to do. It's generating
19 that consensus, I think --

20 Senator Graham: Is there anything Congress is not
21 doing that you would like us to do to help resolve this
22 issue?

23 Admiral Rogers: No, I can't argue that it's something
24 that Congress has failed to do. I don't see that.

25 Senator Graham: Thank you.

1 Admiral Rogers: Sir.

2 Chairman McCain: Senator Hirono.

3 Senator Hirono: Thank you, Mr. Chairman.

4 Admiral, I know that you talked a little about cyber
5 teams in response to our -- to earlier questions. And I
6 think the idea to leverage our outstanding National Guard
7 capabilities and capacity in establishing many of these
8 cyber teams is a good idea. As you and your colleagues
9 look to establish additional cyber units in the future --
10 and while I'm sure you are looking at this region, meaning
11 the Pacific region, I ask that you look closely at the
12 needs of the Asia-Pacific region. In Hawaii, for example,
13 as you well know, we have PACOM, NSA Hawaii, various
14 component commands, and other agency regional officers that
15 are -- offices that are likely targets for cybercriminals
16 and -- you know, as we focus on the rebalance to the Asia-
17 Pacific, obvious. I wanted to get to a question.

18 Last September, the U.S. and China did agree that
19 neither government would support or conduct cyber-enabled
20 theft of intellectual property. Now that we are 6 months
21 down the road, would you say that China is living up to
22 this agreement?

23 Admiral Rogers: Well --

24 Senator Hirono: And I don't know how specific the
25 agreement was, frankly, but, you know, it seemed like a

1 good idea for the two countries to enter into that kind of
2 a dialogue and discussion. But, really, what is happening
3 with regard to that agreement?

4 Admiral Rogers: So, if I could, what the agreement
5 said would -- was, neither nation would engage in that
6 activity for the purpose of gaining economic advantage for
7 their private sector. We continue to see Chinese activity
8 in this regard. The million-dollar question is, Is that
9 activity for governmental purposes or is it being then
10 passed from the government to the private sector? It --
11 from my mind, the jury is still out in that regard. Its
12 activity level is somewhat lower than prior to September of
13 2015.

14 Senator Hirono: But, is there any way that we can
15 determine whether China is engaging in such activity?
16 Really, are there any parameters? Is there anything that
17 we measure to determine whether these -- this agreement is
18 being adhered to?

19 Admiral Rogers: Yes, ma'am. In an unclassified
20 forum, I'm not going to get into the specifics of how we go
21 about doing that, but yes, ma'am.

22 Senator Hirono: So, one of the areas of -- thank you.
23 And maybe in another context, we can get to some of those
24 questions. With regard to our ability to support a -- our
25 cyber capabilities, training and retention, really

1 important. And so, in that regard, STEM education is
2 critical. Can you just talk a little bit more about what
3 you are doing to -- any collaborations, partnerships you
4 are doing with universities or community colleges to train
5 a workforce for us?

6 Admiral Rogers: So, let's just take Hawaii as an
7 example. Today, as a matter of fact, in Kunia, the
8 adjutant general for the Guard in Hawaii is meeting in the
9 Kunia complex with U.S. Cyber Command, NSA, and elements
10 from across the island on Oahu to try to look at -- to
11 include the academic sector -- How do we generate a more
12 capable workforce both to meet Guard requirements as well
13 as to meet Cyber Command, NSA, and other elements? How can
14 we partner more effectively in aligning that capability to
15 deal with issues of common interest to us; in this case, on
16 Oahu, specifically, and the State of Hawaii, in -- more
17 broadly? You see that same -- Hawaii is an area where we
18 probably are -- have gone further than others, but you can
19 see that same type of activity for U.S. Cyber Command right
20 now with what we are doing with a handful of universities
21 across the United States, from the West Coast -- Carnegie
22 Mellon -- there are some West Coast universities, Tulsa,
23 you heard, one -- there's, I want to say, something on the
24 order of 60 to 100 right now, between NSA and Cyber
25 Command. This is one area where NSA and Cyber Command tend

1 to partner together a lot.

2 Senator Hirono: Obviously, that needs to continue,
3 because our cyber capability is something that is going to
4 be an ongoing --

5 Admiral Rogers: Right.

6 Senator Hirono: -- effort.

7 You mentioned the importance of the private sector in
8 a whole-of-government plus, you know, outside-of-government
9 approach to cybersecurity needs. So, how do you envision
10 the private sector's role?

11 Admiral Rogers: So, what we've tried to do at Cyber
12 Command is -- what I think the private sector brings is
13 technical innovation, intellectual innovation, if you will
14 -- just broad knowledge of capabilities -- and alternative
15 ways to look at problems, if you will. Those are, at a
16 macro level, the three things -- when I look at the private
17 sector, I say, "Wow, you really could add value for us in
18 that regard."

19 What we've done to date is, we've created what we call
20 the Point of Partnership in Silicon Valley, where I've
21 placed a very small element on the ground. The part that's
22 interesting to me is, I did not want U.S. Cyber Command
23 people out there. Instead what I wanted was one individual
24 who's a U.S. Cyber Command individual, and then I wanted to
25 harness the power of Reserve individuals who are currently

1 in the ecosystem in the Valley, working in their day-to-day
2 jobs. We've just started that since last summer. That's
3 starting to work out very well for us. It gives us a
4 chance to get a sense for what technical innovation is
5 going on out there. We approach them with different
6 problem sets and say, "Hey, here's an issue we're still
7 trying to work our way through. How are you handling this?
8 Or would you give us some suggestions on how we might deal
9 with it?" I'm trying to see if we can replicate that model
10 that we currently have in place in Silicon Valley in other
11 areas. I'm looking at the East Coast next, kind of as an
12 example of that, probably somewhere in the Greater Boston
13 Metro area next.

14 Senator Hirono: So, it sounds like more of an
15 informal kind of arrangement right now, and maybe, going
16 forward, you would want to maybe institutionalize --

17 Admiral Rogers: Right.

18 Senator Hirono: -- this kind of collaboration with
19 the private sector.

20 Admiral Rogers: Yes, ma'am.

21 Senator Hirono: Thank you, Mr. Chairman.

22 Chairman McCain: Senator Tillis.

23 Senator Tillis: Thank you, Mr. Chairman.

24 Admiral Rogers, I don't envy you with the job that you
25 have, the complexity and then the additional challenges

1 that we have, as the Chairman has said, about
2 sequestration, things that are on the horizon that you have
3 to worry about.

4 The -- you know, and in listening to the discussion, I
5 think one thing that's very important is, we're never going
6 to have the perfect weapon. This is not -- you know,
7 absent the United States coming up with a game-changing
8 offensive or defensive capability of the scale of the
9 Manhattan Project, you can't possibly get inside the
10 decision cycles of the state actors, organized crime,
11 terrorists, and other people. If -- and when you think
12 about decision cycles in this realm, you think about --
13 every single day, you get new malware, viruses, other
14 technology added to your PC to deal with new threats that
15 didn't exist a day or two or a week before. So, I'm trying
16 to get my head around how you really even segregate your
17 scope of responsibility, which is largely, you know, the
18 vulnerabilities of, say, the DOD or with -- however you
19 would --

20 Admiral Rogers: Right.

21 Senator Tillis: -- like to define your scope,
22 ability, and how you differentiate that from the broader
23 private-sector threat. I mean, you've got 28 million small
24 businesses. You have close to 19,000 businesses with 500
25 employers or more. You have distributed public-sector

1 infrastructure, whether it's electric, water, gas. If --
2 and the concern that I have is, what we have right now are
3 the equivalent of guerrilla sniper fire or mortar attacks.
4 We haven't seen -- and I think that we will see someday --
5 a nation-state or organized crime or terrorist organization
6 literally be in a position to execute a multi-pillar attack
7 that, if they're smart -- and they are -- what they will do
8 is something to disrupt you, and then disrupt your ability
9 to react to it by attacking the private sector, which is
10 also integral to your supply chain.

11 So, you know, how are we looking at this on a global
12 basis and understanding that, as they continue to increase
13 their abilities, they're going to figure out a way, on a
14 multi-pillar basis, to go after communications
15 infrastructure, a supply-chain infrastructure, healthcare,
16 electric, whatever public infrastructure may be vulnerable
17 -- how do we actually get these things to coalesce, versus
18 finding out we create -- we get a good job -- we do a good
19 job in DOD, we create the Maginot Line, and they just go
20 around it and disrupt you from a different direction?

21 Admiral Rogers: So, you have very succinctly
22 articulated much of the problem set and the challenges of
23 how you operate in this environment, because the -- these
24 arbitrary boundaries that we traditionally consider, "Well,
25 this is a DOD function and this is a private function, this

1 is an inherently government" -- cyber just blurs these
2 lines. So, even as I focus on the DOD mission, it's one
3 reason why I've argued we have got to think so much more
4 broadly about this problem set.

5 Now, within the DOD arena, it's one of the reasons
6 why, for example, if you look at our exercise in training
7 regime that we've put in place, we try to do that, not just
8 within the DOD, but across a breadth of the private sector.
9 CYBERGUARD is our annual exercise. It'll be in June of
10 this year. We pick a different segment, if you will, every
11 year. We're going to do the power segment in this year's
12 exercise. I think it's something like 20 different
13 corporations will be exercising with us -- the Guard,
14 State, local --

15 Senator Tillis: Well, that's -- you know, that's what
16 I'm getting to. It's almost as if your military exercises
17 have to involve all of these players --

18 Admiral Rogers: Sure.

19 Senator Tillis: -- so that they have a better
20 understanding of their vulnerabilities and the nature of
21 the attack that would occur in cyber.

22 And the other question that I had is, To what extent
23 are we looking at State and local governments as a way to
24 at least -- in North Carolina, I served in the legislature,
25 and we were talking about what we could do to work on

1 cyberthreats. And I saw it also as an economic advantage.
2 If States became particularly good at grid-hardening or at
3 securing the physical presences and cyberthreats within
4 their State borders, they actually create an economic
5 advantage for people to set up business in --

6 Admiral Rogers: Right.

7 Senator Tillis: -- those States. So, to what extent
8 are we trying to lead and help make this problem a little
9 less difficult at the Federal level by making sure that the
10 States and local governments are stepping up their game as
11 a part of the effort?

12 Admiral Rogers: So, it's one of the reasons why
13 there's a big Guard component to this effort, to ensure we
14 can also try to address the State and local aspects of
15 this.

16 Senator Tillis: Thank -- I have a million different
17 questions. I think --

18 Admiral Rogers: Sure.

19 Senator Tillis: -- what I'll probably do is see if I
20 can schedule some time --

21 Admiral Rogers: Oh, yes, sir.

22 Senator Tillis: -- in my office to go over a number
23 of other ones. We may have to do some in a secured
24 setting.

25 Thank you very much.

1 Chairman McCain: Senator Reed.

2 Senator Reed: Thank you, Mr. Chairman.

3 One of the issues is, in fact, sort of the services
4 being able, within their resources, to fully develop the
5 units that they will detach to, essentially, or provide for
6 your operational control, since you won't have your organic
7 units. Can you give an assessment of sort of where we are
8 -- where they are, in terms of doing that, across the
9 services?

10 Admiral Rogers: So, that really goes to the heart of
11 readiness, if you will. And one of the -- so, in
12 September, when I was with you, one of the things I said
13 then, during that session, was that I thought one of the
14 reasons why 16 was going to be such a big game-changer was,
15 I thought we'd get more involved in the total breadth of
16 capability sets, which we are. And then, the other reason
17 was because we needed to shift from a focus on IOC and FOC,
18 the generation of capability, to actual readiness, "Okay,
19 guys, are we actually ready to employ this?" So, we have
20 spent the last 6 months working our way through, How do you
21 define readiness in the cyber arena, down to the individual
22 team level so that I, as a commander, have an awareness of
23 what the true capabilities of the force is, and, using the
24 same mechanisms that we use to assess readiness across the
25 DOD, I can provide policymakers and decisionmakers a true

1 picture of, "This is just -- here is what this force is
2 really capable of doing."

3 We've just started doing that. I've gone through two
4 strawmen so far with the team. We're going to do a third
5 and final one this summer. And then, by the end of the
6 summer, in September, I will start providing to the DOD, on
7 a quarterly basis, by team, "Here's where we are in terms
8 of true readiness."

9 Chairman McCain: Is the nightmare scenario that one
10 of these nations acquires the capability to shut down
11 satellites?

12 Admiral Rogers: I mean, that is a -- there's two
13 scenarios that really concern me. One is the physical
14 shutdown and interdiction of capability. The other
15 scenario that I --

16 Chairman McCain: But, explain the first one.

17 Admiral Rogers: If you were to shut down -- look at
18 it from -- first, from a narrow DOD perspective -- because
19 much of what we rely on for our enablers as a Department
20 are commercial infrastructure -- power, our ability to move
21 force, for example. If you were able to try to take that
22 away or materially impact the ability to manage an air
23 traffic control system, to manage the overhead structure
24 and the flow of communications or data, for example, that
25 would materially impact DOD's ability to execute its

1 mission, let alone the broader economic impact for us as a
2 Nation.

3 The other concern I have is, to date, most
4 penetrations of systems that we've seen by actors have
5 either been to steal data or to do reconnaissance. What
6 happens if the purpose of the intrusion becomes to
7 manipulate the data? And so, you can no longer believe
8 what you are seeing. Think about the implications of that,
9 if you couldn't trust the military picture that you are
10 looking -- that you're using to base decisions on, and let
11 alone the broader economic impacts for us as a Nation.

12 Chairman McCain: Senator Shaheen.

13 Senator Shaheen: Thank you, Mr. Chairman.

14 And thank you --

15 Admiral Rogers: Senator.

16 Senator Shaheen: -- Admiral, for being here and for
17 the job that you're doing every day to protect the country.

18 I wanted to, first, start with a statement you made
19 earlier, I think, to a question from Senator McCain about,
20 Does Russia have the capacity to inflict serious harm to
21 our infrastructure? And you said yes. Do we have capacity
22 to inflict serious harm to Russia's infrastructure?

23 Admiral Rogers: In an unclassified hearing, I'd
24 rather not get into that, if I could, ma'am. I don't --

25 Senator Shaheen: But, I -- let me put it in the

1 context of -- I assume there is some mutual deterrence that
2 goes on when we're talking about some state actors.

3 Admiral Rogers: Again, it's a lot more complicated
4 than just a yes or a no.

5 Senator Shaheen: Okay. Well, I hope that we will be
6 able to ask that question in a --

7 Admiral Rogers: Yes, ma'am.

8 Senator Shaheen: -- classified setting.

9 I had the opportunity, over the last 2 weeks, to visit
10 Estonia, which is, as you know, one of the most wired
11 countries --

12 Admiral Rogers: Right.

13 Senator Shaheen: -- in the world, and also the --
14 probably the first victim of a cyberattack by a nation-
15 state, by Russia. And I had the opportunity to visit the
16 Cyber Center that's been accredited by NATO and to hear
17 them talk about how they think about cyber issues. And can
18 you talk a little bit about how CYBERCOM works with our
19 NATO allies?

20 Admiral Rogers: So, I've been in Tallinn, myself.
21 I've been to the Center. I was just in Brussels, for
22 example, in December, and I -- as U.S. Cyber Command, I
23 addressed the North Atlantic Council, you know, as one of
24 the member nations. I was asked to talk to the leadership
25 of the alliance about implications of cyber and how might

1 the -- just one voice, I'm the first to acknowledge that --
2 how might the alliance work its way forward as we're trying
3 to deal with the cyber arena. Cyber Command, I tried to
4 partner both with the alliance as a whole as well as
5 specific member nations on specific issues within the
6 alliance. What I suggested to NATO is, I think the real
7 key is, you've got to get the defensive house together,
8 number one, and then, secondly --

9 Senator Shaheen: Explain a little more what you mean
10 when you say that.

11 Admiral Rogers: Much like we've seen on the U.S.
12 side, I've said, "Look, I see NATO is spending a lot of
13 time -- and it's a good thing -- focused on defense of
14 NATO's fixed infrastructure," but I also remind them that I
15 think there's value in spending time thinking about -- for
16 example, as NATO is creating additional capability of
17 different, additional force constructs to be able to apply
18 traditional capability in a much faster way. I've also
19 been part of discussions where I remind them, "Even as
20 you're generating that additional force, that additional
21 capability, you need to be thinking about, What are the
22 cyber vulnerabilities and the cyber defense implications of
23 that? Because we can spend a lot of money on generating
24 new capability, but if it's got inherent vulnerabilities
25 that quickly negate its ability to actually be used, that's

1 not a good situation for the alliance or for us. We're
2 dealing with the same challenges. I've had those
3 discussions with the alliance, writ large.

4 Senator Shaheen: And so, how do we increase their
5 participation in training exercises like CYBERFLAG?

6 Admiral Rogers: So, for CYBERFLAG, for example, we
7 have some NATO nations that participate in CYBERFLAG, which
8 is U.S. Cyber Command's largest exercise. I won't say we
9 have all 28 member nations at CYBERFLAG. We -- over time,
10 you'll see more and more nations participating. One of the
11 things I've talked to NATO about, although we haven't yet
12 fleshed out the how, is, How might we go about taking a
13 look at a cyber exercise or training regime? I'd be the
14 first to admit, this is just a preliminary discussion.
15 But, when I was there in December, I said, "Hey, look, I
16 think this is something we need to be thinking about."

17 Senator Shaheen: One of the things that I was really
18 interested in, in Estonia, was hearing about their Estonian
19 Defense League.

20 Admiral Rogers: The Defense League.

21 Senator Shaheen: And you were talking about --
22 earlier in your testimony, about the effort to take
23 advantage of the expertise in the private sector to help us
24 as we're looking at cyber issues. And I was very
25 interested. One of the things I heard was that the reality

1 is, we can't completely prevent a cyberattack. And so,
2 what we've really got to do is be prepared to respond to
3 that attack in the way that is most effective and most --
4 and fastest. And they were talking about their Defense
5 League as one way that they are able to do that. Is that
6 something that -- recognizing that we're probably not
7 talking about -- is -- but, is that what you're looking at
8 when you're talking about the teams that are being set up
9 to help respond?

10 Admiral Rogers: It's a little different, in the sense
11 that the idea behind the Cyber League for Estonia is, you
12 have private citizens --

13 Senator Shaheen: Right.

14 Admiral Rogers: -- who volunteer -- on a voluntary
15 basis --

16 Senator Shaheen: Right.

17 Admiral Rogers: -- will apply themselves at specific
18 problem sets as they emerge, kind of after hours, after
19 work, on their own time. That's kind of the model for the
20 Cyber League in Estonia. And they use that to augment
21 their government and --

22 Senator Shaheen: Right.

23 Admiral Rogers: -- private-sector capabilities.

24 On the U.S. side, for us in the DOD, that Cyber
25 League, I would argue, is a cross, for us in our

1 structures, between the digital service arena that DOD is
2 creating as well as the kind of Guard construct, although
3 the difference is, when the Estonians do it, you're doing
4 it purely on your own time, purely as assistance, not as a
5 uniformed member of the Guard and Reserve, so to speak.
6 So, it -- it's not exactly the same, but the thought
7 process that --

8 Senator Shaheen: Right.

9 Admiral Rogers: -- the idea of trying to tap that is
10 similar.

11 Senator Shaheen: Thank you.

12 Thank you, Mr. Chairman.

13 Chairman McCain: Senator Ayotte.

14 Senator Ayotte: Thank you, Chairman.

15 I want to thank you, Admiral Rogers, for your service
16 --

17 Admiral Rogers: Senator.

18 Senator Ayotte: -- to the country.

19 I wanted to just ask you a basic question. You have
20 substantial responsibility in your position. What keeps
21 you up at night? What are the thing -- what is -- you're
22 most worried about that we need to understand?

23 Admiral Rogers: Well, let me be bit of a smartass and
24 say, based on the workload, I have no problem sleeping.

25 [Laughter.]

1 Admiral Rogers: But, secondly, there's three things,
2 generally, I highlight. Number one is actions taken
3 against critical infrastructure in the United States,
4 damage or manipulation. Number two, what happens when
5 actors start to no longer just enter systems to do
6 reconnaissance or to steal, but actually to manipulate or
7 change data so that we no longer can believe what we're
8 seeing? And the third and final thing in the cyber arena
9 is, What happens when nonstate actors start to use cyber as
10 a weapon system and they want to use it as a vehicle to
11 inflict pain and -- against the United States and others?

12 Senator Ayotte: And to the third point you just made
13 about nonstate actors using cyber as a weapon system, how
14 grave of a threat is that to us, currently?

15 Admiral Rogers: I would argue that it is not -- you
16 know, it's one of these, you say it and then tomorrow
17 something will change. But, today what I would tell you
18 is, I have not seen groups yet make huge investments in
19 this, but I worry that it's a matter of time, because it
20 wouldn't take long. One of the challenges of cyber -- in
21 addition, we've previously talked today about how it
22 doesn't recognize boundaries. It doesn't take billions of
23 dollars of investment. It doesn't take decades of time.
24 And it doesn't take a dedicated workforce of tens of
25 thousands of people, like you see most nation-states deal

1 with. The problem is that cyber is the great equalizer in
2 some ways.

3 Senator Ayotte: And what are the greatest risks, to
4 the extent you can describe them here, to our critical
5 infrastructure, the first issue that you --

6 Admiral Rogers: I just worry -- in that regard, what
7 I worry is -- based on the accesses and the activity that
8 I've seen of some nation-state actors out there, what
9 happens if they decide that they want to, for some period
10 of time, disrupt the things we take for granted, the
11 ability to always have power, pumps --

12 Senator Ayotte: Power system --

13 Admiral Rogers: Power systems.

14 Senator Ayotte: -- financial system.

15 Admiral Rogers: To move money. I mean, if you take a
16 look at the scenario in the Ukraine on the 22nd of
17 December, imagine had a scenario like that unfolded in the
18 United States. I'm not going to argue that someone's
19 capable of making the United States totally go dark, but I
20 would argue there's capability there to cause significant
21 impact and damage.

22 Senator Ayotte: That's why you discussed, in your
23 opening testimony, the need for the coordination between
24 government, private --

25 Admiral Rogers: Yes, ma'am.

1 Senator Ayotte: -- sector, and across the whole of
2 government.

3 Admiral Rogers: Right.

4 Senator Ayotte: I wanted to ask you -- the law that
5 was changed by Congress, in terms of the NSA, the holding
6 of information --

7 Admiral Rogers: Oh, the --

8 Senator Ayotte: -- the USA Freedom Act --

9 Admiral Rogers: -- USA Freedom Act. Yes, ma'am.

10 Senator Ayotte: -- can you give us an update on what
11 is happening with that, and whether that's working, and any
12 concerns you have? I think it's an important question --

13 Admiral Rogers: Right.

14 Senator Ayotte: -- for us to check back in with you
15 on.

16 Admiral Rogers: Yes, ma'am. So, if I could, in an
17 unclass hearing, I'm not going to go into great detail.
18 What I would say is, and what I've said to the intelligence
19 oversight committees, we have been able to comply with the
20 Act, and to do it on time. There has been some level of
21 slowness, but that -- in terms of difference from the old
22 system and the new system -- but that --

23 Senator Ayotte: Terms of how quickly you can get
24 information?

25 Admiral Rogers: -- that's -- right, that's -- that

1 time duration is minutes or hours, it's not days or weeks.
2 So, it hasn't yet gotten to the point where I've felt I've
3 needed to come back to the Congress or the administration
4 and say, "Look, I'm seeing a significant material impact on
5 our ability to generate timely insights." Because I made
6 that commitment. I said if I saw that, then I believe I
7 owe it to the Nation to make that point. I have not seen
8 that yet.

9 Senator Ayotte: But, there's no doubt that it's
10 taking longer, in some ways.

11 Admiral Rogers: In some ways, it takes longer.

12 Senator Ayotte: Well, I think it is important for you
13 to come to us with that, because, you know, given that
14 minutes and hours can make a difference ==

15 Admiral Rogers: Yes, ma'am.

16 Senator Ayotte: -- when it comes to terrorist
17 attacks, and preventing them, and taking action, I think
18 this is really important for all of us to understand, given
19 the world that we are living in.

20 I wanted to ask you a final question about the JCPOA,
21 or the Iran deal.

22 Admiral Rogers: Yeah, the Iran --

23 Senator Ayotte: And in there, there's a provision
24 that said that the U.S. must cooperate with Tehran through
25 training and workshops to strengthen Iran's ability to

1 protect against sabotage of its nuclear program. Admiral
2 Rogers, from a cyber perspective, has the U.S. helped
3 Tehran strengthen its ability to protect against sabotage
4 of its nuclear program --

5 Admiral Rogers: Ma'am, I can't speak --

6 Senator Ayotte: -- this agreement?

7 Admiral Rogers: -- I cannot speak for the U.S.

8 Government as a whole. I can tell you U.S. Cyber Command
9 has not participated in any such effort.

10 Senator Ayotte: Okay. Thank you.

11 Admiral Rogers: Yes, ma'am.

12 Chairman McCain: Senator Kaine.

13 Senator Kaine: Thank you, Mr. Chair.

14 Thank you, Admiral Rogers.

15 Admiral Rogers: Senator.

16 Senator Kaine: And I have missed some of the
17 discussion. I don't want to be needlessly repetitive, but
18 I met -- I want to go back to an interchange that you had
19 with the Chair in the opening questions that he asked -- I
20 met recently with a senior military leader, who kind of
21 tried to, basically, summarize his sense of things, and he
22 said, "We have O-plans, but no strategy." And I've been
23 thinking about that. I think, in your back-and-forth with
24 the Chair, you talked about -- and I think others may have
25 asked you about this a little bit -- this notion that we

1 are kind of reacting case-by-case to cyberattacks, and kind
2 of deciding, in each instance, what we want to do. But,
3 the development of a broader doctrine, whether it's, you
4 know, what will a deterrence policy be that we might
5 communicate, how do we view a cyberattack under Article 5
6 of NATO, in terms of triggering a collective self-defense
7 -- the collective defense obligation -- that we're
8 assessing those things, but we're kind of not at the
9 endpoint of answering a lot of those questions. Could you
10 talk to us about the kind of doctrinal development process
11 and -- in working on these questions, they're so important.
12 What might we expect from the Pentagon, from Cyber Command,
13 in our interaction -- in our oversight -- in terms of the
14 development of doctrines that have greater clarity and that
15 aren't just kind of pragmatically reacting?

16 Admiral Rogers: Right. So, you'll see, in the DOD
17 cyber strategy -- for example, we've got a broad
18 overarching framework for the Department about how we are
19 going to both develop capability and then employ it. We're
20 part -- Cyber Command is part of the broader dialogue
21 within the Department about, How do we align the
22 capabilities of the force with the world that we're seeing
23 today? One of the arguments that we've made over the
24 course of the last 6 months is, we need to take an element
25 of the cyber capability we're generating and focus it very

1 much in the deterrence piece. How do we shape, potentially
2 drive, opponent choices and behavior before we get to the
3 crisis scenario? We're in the early stages of that, but
4 I'm very heartened by the fact that we now have broad
5 agreement that that's an important part of our strategy,
6 and we need to be doing that. So, we're just starting the
7 early stages of that journey.

8 The Department participates in the broader dialogue
9 within the U.S. Government as to about how -- from a
10 national policy perspective, how are we going to move
11 forward in addressing some of the issues that you have all
12 raised today? Meanwhile, for me, as U.S. Cyber Command,
13 what I remind our team is, "We know that capability is
14 going to be part of that deterrence strategy, both offense
15 and defense. Guys, that's what we get paid to do. We have
16 got to focus on generating that capability today." So, we
17 can't wait for this broader discussion to complete itself.
18 That's just a losing strategy for us. So, that's kind of
19 been, if you will, the focus for U.S. Cyber Command, at the
20 operational level that I and the team really focus at.

21 Senator Kaine: Let me ask you another question. And
22 I think Senator Shaheen may have asked this before I came
23 into the room, with respect to NATO. But, another item
24 that's very common in this committee as we talk -- look at
25 the postures of other commands, is joint training

1 exercises. India does more joint training with the United
2 States than any other nation. We have marines deployed
3 throughout Africa in these Special Purpose MAGTFs, doing
4 training of African militaries. What is our posture, vis-
5 a-vis sort of partners, in the cyber area, in the training
6 that we do together, in the development of --

7 Admiral Rogers: Right.

8 Senator Kaine: -- you know, joint resiliency
9 strategies?

10 Admiral Rogers: So, we do some level of training with
11 key allies. One of the challenges for us, quite frankly,
12 is, How do you maximize capacity? So, it's all about
13 prioritization. You cannot do everything you would like to
14 do with every nation that you would like to do it. So,
15 part of our strategy is, How do you focus the greatest
16 return? And what are the nations that you want to start
17 with? So, we have done that.

18 The other challenge I find is -- and this is part of
19 an ongoing internal discussion for us -- based on where we
20 are in the journey right now, I can't do so much with the
21 external world that it negatively impacts our internal
22 ability within the Department to generate. Because, unlike
23 some mission sets, where we literally have decades of
24 infrastructure, capability, capacity, and experience, we
25 don't have that in the cyber arena. So, the same force and

1 capability I'm using to help train and partner with foreign
2 counterparts, I'm still building every day. So, that's
3 part of the challenge for us right now. I don't think
4 it'll be as much an issue in the future as that capacity
5 fully comes online, but we're not there yet.

6 Senator Kaine: We trained aviators out of other
7 service branches, and then we created an Air Force Academy
8 in 1954 and decided, okay, we're going to, you know, train
9 aviators at -- not that we don't train aviators in the
10 other service branches. I think --

11 Admiral Rogers: Right.

12 Senator Kaine: -- Senator McCain may have had some
13 training somewhere in his past. But, we created an Air
14 Force, you know, after World War II. I've wondered about
15 whether the cyber domain would eventually become so
16 significant that there may be the need to consider creating
17 a dedicated Cyber Academy, much like the Air Force was
18 created in the '50s. Now the question is, you can train
19 cyber folks everywhere and have them percolate throughout
20 the service branches, or you can focus on a particular
21 cyber expertise, and then those folks could go into the
22 different service branches. Have -- has there been any
23 discussion or thought about that?

24 Admiral Rogers: I mean, it's been a discussion. My
25 input to that discussion has been, I'm not, right now,

1 based on my experience and what I see, a proponent of that
2 approach. Because my concern is, to maximize effectiveness
3 in cyber, you need to understand how it fits in a broader
4 context. And I watch, at times, when I deal with elements
5 in our own workforce who are incredibly technically savvy,
6 incredibly smart about other eaches of the mission, and
7 yet, when I try to remind them, "Remember, we're applying
8 this as part of a broader strategy and a broader context"
9 -- when you don't understand that broader context, you're
10 just not -- in my experience, you're not as effective.
11 And that's my concern about that approach. It'll start to
12 really make us very, very --

13 Senator Kaine: Siloed.

14 Admiral Rogers: -- narrow and siloed. And I'm just
15 concerned about the potential implications of that.

16 Senator Kaine: Great. Thank you.

17 Thanks, Mr. Chair.

18 Chairman McCain: Senator Cotton.

19 Senator Cotton: Admiral Rogers, thank you for
20 appearing again before --

21 Admiral Rogers: Sir.

22 Senator Cotton: -- the committee.

23 If I heard you correctly, you testified to Senator
24 Ayotte that your three main fears were threats to our
25 critical infrastructure, the ability to manipulate systems

1 such that we might not have faith in their operations, and,
2 third, nonstate actors using cyber as a weapon against the
3 United States. Is that an accurate --

4 Admiral Rogers: Yes, sir.

5 Senator Cotton: Yeah. Are --

6 Admiral Rogers: Yes, sir.

7 Senator Cotton: Are either the Islamic State or al-
8 Qaeda able to do any of those three things at this point?

9 Admiral Rogers: I haven't seen them yet, but my
10 concern is, that's now.

11 Senator Cotton: So, the Islamic State has a
12 reputation for being very effective online. Can -- what we
13 infer, then, is online recruiting and propaganda is a
14 distinct skillset from the use of cyber as a weapon --

15 Admiral Rogers: Yes, sir.

16 Senator Cotton: -- against things like electrical
17 power grids and so forth.

18 Admiral Rogers: Yes, sir.

19 Senator Cotton: How hard would it be for a nonstate
20 actor, like the Islamic State or al-Qaeda, to develop that
21 skillset? Is it nothing more than recruiting the right
22 person?

23 Admiral Rogers: It would not be difficult. It's
24 about recruiting the right people with the right focus, but
25 it would not -- it's certainly not beyond their ability if

1 they decide -- I believe it's not beyond their ability if
2 they made that decision.

3 Senator Cotton: When we think about other potential
4 nonstate actors, are those -- do those groups that have
5 that capability or are approaching the capability tend to
6 be associated with state actors?

7 Admiral Rogers: In some cases, yes, but not in all.
8 Not in all.

9 Senator Cotton: Okay.

10 I want to turn now to the ongoing debate about
11 encryption. I think data security and cybersecurity is
12 obviously critical in the modern world. Most people in
13 this room probably have a smartphone in their pocket. Even
14 my 70-year-old father finally turned in his flip phone and
15 got a smartphone recently. We keep emails, text messages,
16 phone calls, financial information, health information, and
17 many other sensitive data --

18 Chairman McCain: He's ahead of Senator Graham.

19 [Laughter.]

20 Senator Cotton: -- on our phones. So, I think data
21 in cybersecurity is essential. I also think physical
22 security is essential.

23 Admiral Rogers: Right.

24 Senator Cotton: And I'd hate to see Americans get
25 blown to pieces because we had an imbalanced priority of

1 cybersecurity over physical security. How do we strike
2 that balance as a society?

3 Admiral Rogers: I -- my first comment would be, I
4 don't think it's either/or. And --

5 Senator Cotton: I don't either. There has to be some
6 kind of --

7 Admiral Rogers: -- my argument would be, we don't
8 serve either viewpoint particularly well when we cast this
9 as, "Well, it's all or nothing, it's either/or." My view
10 is, over time, we have been able to integrate ground-
11 changing technology in the course of our Nation, and to do
12 it in a way that enables the Nation, under the right
13 circumstances, with the right level of control, to be able
14 to access that. For me, my starting position is, What is
15 it that is different about this that would preclude that
16 from applying here? I just don't personally see that, even
17 as I acknowledge there's no one simple answer, there's
18 probably no one silver bullet. It's not going to be a one-
19 size-fits-all. But, I look at the innovation and the can-
20 do approach that we have as a Nation to this, and I'm
21 thinking we can't -- we can solve this.

22 Senator Cotton: Like, for instance, a decades-old law
23 known as the Communications Assistance for Law Enforcement
24 Act --

25 Admiral Rogers: Act.

1 Senator Cotton: -- which tells telecom companies of
2 any size that if they want to construct a telephone system
3 in this country, it has to be susceptible to a wiretap,
4 pursuant to a court order, if a court finds probable cause
5 to order a wiretap against a terror suspect or a human
6 trafficker or a drug dealer or so forth. Similarly, we all
7 expect privacy in our bank accounts, but banks, obviously,
8 must maintain systems in which they turn over bank account
9 information, subject to a court order, against, say, a
10 potential money launderer. Is there any reason our society
11 should treat data and tech companies differently from how
12 we treat telephone companies and banks?

13 Admiral Rogers: I mean, that's clearly a much broader
14 issue than Cyber Command. I won't get into the good or
15 bad, so to speak, but I -- like you, I'd just say, "Look,
16 we've got frameworks in other areas. Why can't we apply
17 that here?"

18 Senator Cotton: Okay.

19 These questions have been about the larger debate
20 about encryption, going forward, the way smartphones are
21 designed, the way messaging systems are designed. There
22 was a case recently, involving Apple and the FBI and the
23 San Bernardino shooter, in which the FBI requested Apple's
24 assistance to override a feature of an iPhone, Apple
25 refused, the FBI apparently found a third party capable of

1 doing so and has withdrawn that case. Should Americans be
2 alarmed at this kind of vulnerability in a -- such a widely
3 used device?

4 Admiral Rogers: The way I would phrase it is,
5 vulnerability is an inherent nature of the technical world
6 that we live in today. And if your desire is to live in a
7 world without vulnerability, I would say that is probably
8 highly unlikely.

9 Senator Cotton: Do you know if we have shared that
10 vulnerability with Apple -- the United States --

11 Admiral Rogers: As U.S. Cyber Command, I -- sir, I
12 apologize, I don't know.

13 Senator Cotton: Thank you.

14 Chairman McCain: Admiral, one other point. We know
15 for a fact that Baghdadi is sending young men into the
16 refugee flow to commit acts of terror wherever they can
17 locate. Is it true, or very likely, that they also know of
18 a Web site to come up on, secure, so that they can
19 communicate back with Baghdadi and his tech --

20 Admiral Rogers: Yes.

21 Chairman McCain: So, right now -- there was a media
22 report that 400 young men had been sent into the refugee
23 flow. I would assume, then, that at least some of them
24 have -- are armed with a Web site to come up on once they
25 get to a preferred destination so that they can coordinate

1 acts of terrorism.

2 Admiral Rogers: A Web site or an encrypted app. Yes,
3 that's probably likely.

4 Chairman McCain: That's a bit concerning, isn't it?

5 Admiral Rogers: Yes, sir.

6 Chairman McCain: So, what should we be doing to
7 counter that?

8 Admiral Rogers: So, I --

9 Chairman McCain: Besides take out ISIS.

10 Admiral Rogers: I think we need a broader national
11 dialogue about, What are we comfortable with? It's not
12 either/or. Because we have got to have security, and we've
13 got to have safety and privacy. And, at the moment, we're
14 in a dialogue that seems to paint it as, well, it's one or
15 the other. And I -- as the dialogue we just had with
16 Senator Cotton, I don't see it that way.

17 Chairman McCain: And yet, we know of a direct threat
18 of an attack in Europe or the United States and a technical
19 capability to enhance their ability to commit this act of
20 terrors.

21 Admiral Rogers: Yes, sir.

22 Chairman McCain: Isn't that a pretty tough -- so, we
23 need a national conversation? Do we need more hearings?
24 Do we need to urge the administration to come up with a
25 policy? What are our options, here?

1 Admiral Rogers: Well, the worst-case scenario, to me,
2 is, we don't have this dialogue and then we have a major
3 event. And in the aftermath of a major event, we decide to
4 do something that perhaps, in the breadth of time, we step
5 back and ask ourselves, How did we ever get here?

6 Chairman McCain: I don't think there's any doubt
7 that's a likely scenario.

8 Admiral Rogers: That is what I hope it doesn't come
9 to. But, to date, for a variety of reasons, we just have
10 unable -- been unable to achieve that kind of consensus.
11 But, we have got to figure out how we're going to do this.
12 And you don't want a law enforcement -- I believe you don't
13 want a law enforcement individual or an intelligence
14 individual dictating this, just as I don't believe you want
15 the private sector, a company, dictating this. This is too
16 important, from my perspective.

17 Chairman McCain: I don't -- we -- is awareness of
18 this threat important to -- for the American people to know
19 how serious this threat is?

20 Admiral Rogers: Yes.

21 Chairman McCain: Senator King.

22 Senator King: Mr. Chairman, it -- hearing this
23 dialogue and the discussion you have just been having, it
24 strikes me it underlines the foolishness of continuing to
25 be governed by budget decisions made 6 years ago, when this

1 threat was nothing like the magnitude that it is today.
2 And here we are, dealing with a major new threat and trying
3 to fit it within -- to shoehorn it within a budget
4 structure that was -- that clearly did not take account of
5 the fact that we've got a major new threat, and a serious
6 one, that we're facing that's going to take resources to
7 confront. It just -- I just can't help but make that
8 point, that it underlines the fact that we're trying to --
9 we're governed by decisions made at a time when
10 circumstances were very different than they are today.

11 Chairman McCain: Well, I thank Senator King. But,
12 Admiral Rogers has already made it clear, I think, in this
13 testimony, that sequestration will prevent him from
14 carrying out completely the missions that he's been tasked
15 with.

16 Is that correct, Admiral?

17 Admiral Rogers: Yes, sir. And my greatest concern,
18 if you went to sequestration, would be the impact on the
19 workforce, particularly the civilians, who would argue,
20 "So, is this what I want to be aligned with?" That concern
21 -- I can replace equipment. It takes us years to replace
22 people.

23 Chairman McCain: And there is a real likelihood that,
24 if we continue the sequestration, that you will have to --
25 you will not be able to continue to employ these

1 outstanding and highly selected individuals.

2 Admiral Rogers: Yes.

3 Chairman McCain: You know, sometimes, Admiral, I do
4 not want the American people to see what goes on at these
5 hearings. The old line about laws and sausages. But, I
6 certainly wish the American people could hear and see your
7 statements that you're making today rather than, as you
8 just indicated, an attack, and then we always overreact,
9 that that's just what democracies are all about.

10 And so, I thank you for your good work, but I also
11 want to thank you for your straightforward answers to
12 questions that were posed by the members of this committee.
13 And we thank you.

14 Hearing is adjourned.

15 [Whereupon, at 11:32 a.m., the hearing was adjourned.]

16

17

18

19

20

21

22

23

24

25