HEARING TO RECEIVE TESTIMONY ON

UNITED STATES CYBER COMMAND IN REVIEW OF THE

DEFENSE AUTHORIZATION REQUEST FOR FISCAL YEAR 2019

AND THE FUTURE YEARS DEFENSE PROGRAM

Tuesday, February 27, 2018

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

The committee met, pursuant to notice, at 9:30 a.m. in Room SH-216, Hart Senate Office Building, Hon. James M. Inhofe, presiding.

OPENING STATEMENT OF HON. JAMES M. INHOFE, U.S. SENATOR FROM OKLAHOMA

Senator Inhofe: The committee meets today to hear Admiral Mike Rogers -- you know, you have more titles than anybody else down here, you really do -- as the Commander of the --

Admiral Rogers: I have that going for me, sir.

Senator Inhofe: -- Commander of the U.S. Cyber Command, Director of the National Security Agency, and Chief of the Central Security Service. And, given your upcoming retirement, it might be this is the last time you'll be dropping in. Is -- do you think that will happen? We'll miss you.

Well, the -- as the recent National Defense Strategy identified renewed great power and competition with Russia and China -- and that kind of stands -- goes along with what General Dunford said when he said that we are losing our qualitative and quantitative edge as we move into this 32 -- or, this 23 National Defense Strategy. As we approach the eighth anniversary of Cyber Command, we should recognize the remarkable progress you've made in taking what was a very niche warfighting concept and establishing around it a full-fledged warfighting command. Later this year, we anticipate that you will achieve full operational capability of -- for the 6,200-person Cyber Mission Force.
Despite the many successes, there are still significant challenges. The committee remains concerned about a hollow cyber force due to the lack of priority across the services to deliver the required tools and capabilities and personnel. Efforts have improved, but the fact remains that we have not -- are not where we need to be, and that we lack the bench strength necessary.

And the other area -- and then I'll have some questions about this during our question time -- is the fact that we're at -- I think, at somewhat of a disadvantage with responsibilities that are spread, as I mentioned to you a few minutes ago, across DOD, DHS, and the FBI, with little semblance of coordination. We can't just wait for a major cyberattack and then try to get this thing right. If we look at some of the other countries, that they have got this more centralized and coordinated. So, we need to address that to see if maybe we've got some improvements that we can make structurally.

Senator Reed.
STATEMENT OF HON. JACK REED, U.S. SENATOR FROM RHODE ISLAND

Senator Reed: Well, thank you very much, Mr. Chairman. And, Admiral Rogers, welcome. And since we are holding the confirmation hearing for your successor later this week, this is likely your last appearance before the committee. Let me thank you for decades of service to the country, to the NSA and Cyber Command. You've done an extraordinary job. Thank you, sir.

One of the great threats facing our democracy is influence operations, a type of information warfare which are mostly conducted through cyberspace, the domain and theater of operations of Cyber Command. Russia engaged in a sophisticated influence campaign during the 2016 election cycle. China has been engaged in information operations against their own citizens in order to control their access to information and their behavior, and is becoming more active abroad. They have also engaged in massive theft of intellectual property conducted against U.S. companies for their own economic gain. North Korea's attack on Sony America was an attempt to silence an entertainment company from exercising its right to free speech and thereby send a message across the world. These efforts by our adversaries highlight some of our vulnerabilities in this area, which I hope you will address today.
While our adversaries are freely conducting information operations, Cyber Command is still predominantly designed to conduct technical operations to either defend or attack computer systems, to sustain or impede the function of computers and networks. It is not built to deal with the content of the information flowing through cyberspace with the cognitive dimension of information warfare. Cyber Command has made important strides in the last year in the cognitive dimension in the struggle against ISIS, but still has a long way to go, and must also focus on the strategic level of engagement, not merely an operational tactical support to engage forces.

Other organizations and officials in the Defense Department are responsible for what the Department calls "psychological and deception operations." But, those officials and departments, in turn, have no expertise or capabilities in the technical aspects of cyberspace operations. This is a serious handicap when we are confronted with adversaries, like Russia, that conduct information warfare that combines the technical and cognitive dimensions to manipulate perceptions through cyberspace. Because we have separated these things organizationally and in terms of policy and strategy, we are greatly disadvantaged when it comes to countering an adversary's integrated operations and when it comes to...
conducting our own information operations through
cyberspace.

The FY18 NDAA included a provision, cosponsored by
Senator McCain and myself, which directs the Secretary of
Defense to designate a senior official to lead the
integration of all Defense Department components and
capabilities that contribute to information warfare, and to
develop specific strategies, plans, and capabilities to
operate effectively in this arena to counter and deter
adversaries. I'm eager to learn how Cyber Command is
responding to this legislation.

As stressed in the newly released National Defense
Strategy, Russia and other adversaries have mastered the art
of conducting a systematic aggression against the United
States and its interests and allies by staying just below
the level that would be considered armed aggression or an
act of war. As the DNI testified recently to the Senate
Intelligence Committee, adversaries are using cyber
operations to achieve strategic objectives, and will
continue to do so unless they face clear repercussions.
Adversaries are achieving strategic effects incrementally by
applying constant pressure through cyberspace against the
sources of our national power.

In addition to tools such as sanctions, diplomacy,
indictments, and public shaming, we must meet not only
Russia, but all adversaries, where the struggle is taking place in the information sphere. As part of this, we need to engage in blunt information operations against us at their source by disrupting them in cyberspace as they unfold.

The National Mission Teams of the Cyber Mission Force were created to conduct exactly these missions. According to Defense Department's official cyberstrategy, the National Mission Teams were created to defend the country by disrupting ongoing cyberattacks of, quote, "significant consequence." Some of these influence operations in cyberspace are directed against the foundations of American democracy: the free expression of Americans' political views, the voting booth, and through our political parties and campaign organizations. Surely, such acts meet the threshold of "significant consequences" justifying the use of the National Mission Teams under the Defense Department's cyberstrategy.

The members of the Cyber Subcommittee, led by Senators Round and Senator Nelson, have made this point numerous times. And I want to thank them for their leadership on the issue. Admiral Rogers, I'm also interested in your views on this issue.

Finally, I understand that presidential leadership is critical on these issues. I raised this matter with the
Director of National Intelligence and each of the intelligence agency directors, including you, Admiral Rogers, at a recent public hearing of the Intelligence Committee. The very disappointing answer that I received is that the President has not corrected any action on countering these threats. In addition, countering these threats requires not only the Defense Department to integrate all the components of information warfare, it is essential to integrate capabilities and authorities of all the national security and law enforcement organizations across the government as a whole. This, too, requires leadership that, so far, has been lacking.

Admiral Rogers, thank you again for your service and the your service of your family. And I look forward to your testimony.

Senator Inhofe: Thank you, Senator Reed. I, regretfully, say that Senator Rounds, who does chair the Subcommittee, will not be here today, or actually this week. He -- with the loss of his father.

Senator Reed: Oh. Sorry.

Senator Inhofe: So, we all regret that.

Admiral Rogers.
STATEMENT OF ADMIRAL MICHAEL S. ROGERS, USN,
COMMANDER, UNITED STATES CYBER COMMAND; DIRECTOR, NATIONAL
SECURITY AGENCY; AND CHIEF, CENTRAL SECURITY SERVICES

Admiral Rogers: Thank you, sir.

Chairman Inhofe, Ranking Member Reed, and distinguished
members of the committee, thank you for your enduring
support and the opportunity to talk with you today about the
hard-working men and women of United States Cyber Command.

But, first, I'd like to take a moment to extend our
thoughts and prayers to Chairman McCain and his family, and
to voice our support for him as he undertakes this tough
health fight. Senator McCain, keep fighting. Look forward
to you getting back, sir.

On behalf of the men and women of the United States
Cyber Command, I'm here to discuss the Command's posture and
describe how we prepare for and execute operations in the
cyberspace domain to support the Nation's defense against
increasingly sophisticated and capable adversaries.

The cyberspace domain that existed when we first
established Cyber Command, nearly -- over 8 years ago, has
evolved dramatically. Today, we face threats that have
increased in sophistication, magnitude, intensity, volume,
and velocity, threatening our vital national security
interests and economic well-being. China and Russia, whom
we see as peer or near-peer competitors in cyberspace,
remain our greatest concern. But, rogue regimes, like Iran
and North Korea have growing capabilities and are using
aggressive methods to conduct malicious cyberspace
activities.

Further, several states have mounted sustained
campaigns against our cleared defense contractors to scout
and steal key enabling technologies, capabilities, and
systems. Our adversaries have grown more emboldened,
conducting increasingly aggressive activities to extend
their influence without fear of significant consequence. We
must change our approaches and responses here if we are to
change this dynamic.

While the domain has evolved, Cyber Command's three
missions areas endure. Our first priority is the defense of
the Department of Defense Information Network, or the DODIN.
Second, we enable other joint force commanders by delivering
effects in and through cyberspace. Finally, we defend the
Nation against cybthreats through support to DHS and
others when directed to do so by the President or the
Secretary of Defense. In concert with the National Defense
Strategy, we are charting a path to achieve and sustain
cyberspace superiority, to deliver strategic and operational
advantage and increased options for combatant commanders and
policymakers. Without cyberspace superiority in today's
battlefield, risk to mission increases across all domains
and endangers our security.

Since my last update almost a year ago, Cyber Command has achieved a number of significant milestones. First, Joint Force Headquarters DODIN, our subordinate headquarters responsible for securing, operating, and defending the Department's complex IT infrastructure, has achieved full operational capability. Second, Joint Task Force Ares, the organization we created to lead the fight in cyber against ISIS, has successfully integrated cyberspace operations into that broader military campaign, and achieved some excellent results. We will continue to pursue ISIS in support of the Nation's objectives. Third, we've significantly enhanced our training and cyber operation platforms to prepare the battlespace against our key adversaries.

And this year will bring several additional accomplishments. Cyber Command will be elevated to a unified combatant commander when I step down, later this spring. As a combatant command, we will have the unique responsibilities of being a joint force provider and a joint force trainer responsible for providing mission-ready cyberspace operations forces to other combatant commanders and ensuring that joint cyberforces are trained to a high standard and remain interoperable.

In addition, in April, we'll start moving into a state-of-the-art integrated cyber center and joint operations
facility at Fort Meade. This will be our first fully integrated operations center that enhances the whole-of-government coordination and improves planning and operations against a range of growing cyberthreats.

Within this dynamic domain, it's imperative to continually evolve the training and tools of our operators. And we've recently delivered the first of several foundational toolkits designed to enable the Cyber Mission Force to work against adversary networks while reducing the risk of exposure, as well as equipping JTF Ares in its fight against ISIS with capabilities designed to disrupt adversary use of the Internet.

Innovation and rapid tech development demand competition and the ability to leverage all partners, including small businesses. We intend, in the coming year, to create an unclassified collaboration venue where businesses and academia can help us tackle tough problems without needing to jump over clearance hurdles, for example, which, for many, are very difficult barriers. Of course, all these tools require a talented and sophisticated workforce to operate and employ them. The Cyber Excepted Service will help us recruit, manage, and retain cyber expertise in a highly competitive talent market.

Our success also remains entwined with continued integration of the Reserve and National Guard. In our
headquarters alone, we currently employ more than 300 full-time and part-time reservists, and, in addition, more than 150 Reserve and National Guard members are mobilized to lead and execute cyberspace operations. For most -- perhaps most significantly, we are nearing completion of the buildout of our Cyber Mission Force, with all teams on a glide path to reach full operational capability before the end of this fiscal year. As the teams reach FOC, our focus is shifting beyond the build to ensuring that those teams are ready to perform their mission and to execute sustained and optimized mission outcomes for the Nation year after year for a sustained effort over time.

And I fully realize that cybersecurity is a national security issue that requires a whole-of-government approach that brings together not only government, departments, agencies, but also the private sector and our international partners. And, over the last year, we've also increased our interaction with critical infrastructure elements within the private sector and the broader set of U.S. Government partners supporting them.

And, as you know, I serve as both Commander of the United States Cyber Command and Director of the National Security Agency. This dual-hat appointment underpins the close relationship between these two organizations. The Fiscal Year '17 National Defense Authorization Act included
a provision that describes the conditions for splitting or
effecting the dual-hat arrangement, and the Department is
working its way through this question; and ultimately the
Secretary, in conjunction with the DNI, will provide a final
recommendation to the President. All of us at Cyber Command
are proud of the roles we play in our Nation's cyber efforts
and are motivated to accomplish our assigned missions
overseen by the Congress, particularly this committee.

And, finally, after serving over 4 years as the
Commander of Cyber Command, and after nearly 37 years of
service as a naval officer, I'm set to retire later this
spring, and I will do all I can during the intervening
period to ensure the mission continues, that our men and
women remain ever motivated, and that we have a smooth
transition. And I'm grateful for the committee's continued
support and confidence of myself and the Cyber Command team,
and I look forward to answering your questions today.

[The prepared statement of Admiral Rogers follows:]
Senator Inhofe: Thank you, Admiral Rogers.

Well, in my opening statement, I addressed this -- the three agencies' approach that we have responsible for defending against the attacks. We have the FBI as the lead for law enforcement; the Department of Homeland Security is the lead for critical infrastructure and defending government computer networks; and, thirdly, the Department of Defense as the lead for defending the homeland, defending military computer networks, and developing and employing military cyber capabilities. So, you've got the DOD, the DHS, and the FBI. No one agency -- no one agency -- has all the authorities required to defend and protect the homeland. So, did we set it up wrong to start with? What does need to be done to encourage a more whole-of-government -- you mentioned that in your opening statement -- combating the cyberthreats that are out there?

Admiral Rogers: So, I think the challenge, as I look at the problem set -- and I'm looking at it from the perspective of an operational commander -- How do we execute and generate outcomes, if you will? I think it's less an issue of people not understanding what their respective roles are within the structure you outlined. And instead, I think the challenge is, How do we integrate those capabilities into a tighter hole, if you will, that's really optimized to execute at the day-to-day level? I think
that's the area where I look at the future, and, as I -- you
know, during my -- with my responsibilities as Commander of
Cyber Command, that's where I'd like to see us focus our
efforts. How do we get down to integrated structures and
organizations at the execution level? Because that's where
you get speed. And one of the challenges with the current
structure -- as I said, while I think people understand
their respective roles, it is not optimized for speed and
agility. And one of the things that I see in the world
we're living in right now, we have got to get faster and we
have got to be more agile.

      Senator Inhofe: Yeah. The -- there's a lot of
discussion about the gaps and seams that exist between each
leg of the whole-of-government approach. Now, our
adversaries will seek to exploit those gaps and seams, and
the confusion that follows an attack as various agencies and
departments grapple with the scatter of authorities needed
to respond. What are the most dangerous gaps and seams, as
you look at them?

      Admiral Rogers: So, for right now, the time it takes
to deploy capability, the time that it takes to coordinate a
response across multiple organizations, when those well-
meaning and hard-working organizations are existing in
separate structures, that's not optimized for speed. And,
to me, what I think the biggest challenge for us is, How do
we integrate this more at an execution level? I understand there's a broader policy issue here, and a broader legal framework. And that's not my role as an operational commander. But, where I see the need for speed and agility is really when it gets down to --

Senator Inhofe: Is someone working on that now?

Admiral Rogers: Oh, there's an ongoing dialogue about, So what's the right way ahead? Now, again, I'm the operational commander, so I have a voice in that --

Senator Inhofe: Maybe we have too many people in that.

Admiral Rogers: -- in that process. And there's no lack of opinions on this topic.

Senator Inhofe: Yeah. Lastly, you had said previously -- and I'm quoting now -- "Offensive cyber, in some ways, is treated almost like nuclear weapons, in the sense that their application outside of defined area of responsibilities is controlled at the chief executive level; it is not delegated down." Has anything changed under this new administration --

Admiral Rogers: So, we're currently -- again, I don't want to speak for the policy side, but I will acknowledge we are currently in a policy discussion on this very issue. You know, the Secretary of Defense has been very aggressive in articulating this concerns him. There's an ongoing discussion at the moment that I hope is going to come to a
way ahead in the near term. Again, I will get an input into
that, as the operational commander. I'm not the primary
decisionmaker, here. I understand what my role is.

Senator Inhofe: All right, good.

Senator Reed.

Senator Reed: Well, thank you very much, Mr. Chairman.
Again, thank you, Admiral Rogers, for not only your
testimony, but your service.

I have a series of questions, and I think they require
just, sort of, yes-or-no answers.

The mission of National Mission Teams under DOD
cyberstrategy is to blunt cyberattacks against the United
States of, quote, "significant consequence." Is that
accurate?

Admiral Rogers: Yes.

Senator Reed: Okay. The Russia's --

Admiral Rogers: Although, if I could, I'd phrase it
as, that's an accurate mission for Cyber Command. We
haven't actually defined it specifically down on the team
level. But, I understand the point you're trying to make, sir.

Senator Reed: Now, is Russia's ongoing campaign to
steal and leak confidential information from our candidates'
political parties to plant and amplify misinformation in
social media, to break into State election board networks,
of significant consequence to our national security?

Admiral Rogers: Certainly, if successful.

Senator Reed: Yes. Do you agree with the DNI Coats' testimony that they will continue to conduct cyber operations to achieve strategic objectives unless they face clear repercussions?

Admiral Rogers: Yes, sir, that was my testimony, as well, in that hearing.

Senator Reed: Is Russia attempting to achieve its strategic objective by influencing U.S. public opinion in elections?

Admiral Rogers: Yes, sir, I believe they are attempting to undermine our institutions.

Senator Reed: Now, aside from our intelligence agencies operating under a presidential finding, are there any other organizations, other than the Cyber Command's Cyber Mission Forces, that have the authority and capability to disrupt Russian election hacking operations where they originate? Does the FBI, DHS, or the States, the private sector, have such authorities or capabilities?

Admiral Rogers: You could argue, probably, only that -- again, that there's a legal aspect to this that I'm not the most qualified -- but, probably you'd argue some combination of DOD/DOJ have the standing authority in that regard.
Senator Reed: But, the mission teams, particularly at the origin of these attacks, have the authority to do so.

Admiral Rogers: If granted the authority. And I don't have the day-to-day authority to do that. If granted the authority.

Senator Reed: So, you would need, basically, to be directed by the President, through the Secretary of Defense --

Admiral Rogers: Yes, sir, as I -- in fact, I mentioned that in my statement.

Senator Reed: Have you been directed to do so, given the strategic threat that faces the United States and the significant consequences you recognize already?

Admiral Rogers: No, I have not. But, if I could flesh this out, I'll say something in an open, unclassified. I'd be glad to go into more detail --

Senator Reed: Yes, sir.

Admiral Rogers: -- in a classified.

Based on the authority that I have as the Commander, I have directed the National Mission Force to begin some specific work -- I'd rather not publicly go into that --

Senator Reed: Right.

Admiral Rogers: -- using the authorities that I retain as a commander in this mission space.

Senator Reed: So, it's inherent ability of a commander
to prepare, plan --

Admiral Rogers: Yes, sir.

Senator Reed: -- and structure. But, you need the -- you need direct authority of the President, through the Secretary of Defense --

Admiral Rogers: To do some specific things.

Senator Reed: Some specific authority.

Admiral Rogers: There are some things I have the authority, and I am acting within that authority now --

Senator Reed: But, where you -- essentially, we have not taken on the Russians yet. We're watching them intrude in our elections, spread misinformation, become more sophisticated, try to achieve strategic objectives, as you have recognized, and we're just, essentially, sitting back and waiting.

Admiral Rogers: I don't know if I would characterize it as "we're sitting back and waiting," but I will say it's probably -- and again, I apologize, I don't want to --

Senator Reed: Right.

Admiral Rogers: -- get into the classified here -- it's probably fair to say that we have not opted to engage in some of the same behaviors that we are seeing, if I could just keep it --

Senator Reed: No, I -- it's -- one searches for, sort of, historical analogies, but, you know, we have, in the
past, seen threats building, but, at some point,
particularly when they've manifested --

Admiral Rogers: Sir.

Senator Reed: -- themselves, which they already have
in 2016, we've taken action, that we've not just continued
to watch.

Admiral Rogers: Right. No, we are doing some things.

Senator Reed: Let's go back to the -- brief time I
have remaining -- the issue that is, I think, consistent
throughout your testimony and the Chairman's comments. And
that is, the technological aspects, which you do pretty
well, and the cognitive issues, you know, the message versus
the medium, we are all over the place, in terms of
fragmentation. Is there any effort to pull that together?
And let me, maybe, focus on a specific point. You know,
you're trying, within DOD, to sort of get everybody lined
up, then the SECDEF and the administration are trying to
line up all the other parts. There's one -- and I -- from my
experience in banking, the Treasury Department has a --
which is designed to do -- be disruptive of financial
transactions, designed to -- you know, it's not just ideas,
it's money that motivates the --

Admiral Rogers: Yes, sir. Yes, sir.

Senator Reed: So, in your view, are you coordinating
with them adequately? Two, do they have adequate resources
on their own to be an effective force to disrupt illegal
financing and to monitor sanctions?

Admiral Rogers: So, I'm not knowledgeable enough about
the specific level of capability and resources, but I will
say we, both Cyber Command and NSA as well, spend a lot of
time working with our Treasury counterparts about developing
insights and knowledge through cyber and other means that
give them insight that enable them to take action.

Senator Reed: Do you think they're effective?

Admiral Rogers: Oh, I think the economic broader
efforts that I've seen undertaken are positive. And you've
seen them against a wealth -- a host of actors out there.

Senator Reed: Thank you.

Senator Inhofe: Since a quorum is now present, I'd ask
the committee consider a list of 1288 pending military
nominations. All of these nominations have been before the
committee the required length of time.

Is there a motion to favorably report this list of 1288
pending military nominations?

Senator Reed: So move.

Senator Wicker: Second.

Senator Inhofe: Okay, second.

All in favor, say aye.

[A chorus of ayes.]

Senator Inhofe: Opposed, no.
[No response.]

Senator Inhofe: The motion carries.

Senator Ernst.

Senator Ernst: Thank you. Thank you, Mr. Chair.

Admiral Rogers, in your opening statement, you rightly noted the importance of National Guard and Reserve cyber warriors. And many of those young men and women bring critical cyber skills from the private sector. Very, very important. However, you don't mention how or if the DOD plans to track cyber capabilities found in the National Guard and Reserve Force. And we've had this discussion before. But, in 2016, the Government Accountability Office report found that, quote, "National Guard units have developed capabilities that could be used, if requested and approved, to support civil authorities in a cyber incident. However, the Department of Defense does not have visibility of all National Guard units' capabilities for this support," end quote.

Last year, I introduced legislation, along with my committee colleagues, Senators Gillibrand and Senator Fischer, to correct this oversight. Unfortunately, it wasn't included in the final version of the 2018 NDAA. And, as of July of 2017, DOD has not complied with the GAO's recommendation.

So, sir, how do you ensure Cyber Command is fully
tapping into the expertise of our National Guard and Reserve units when the DOD doesn't have visibility of all of the capabilities within the National Guard? And what more can we do to correct this at Cyber Command?

Admiral Rogers: So, I try to work closely with General Lengyel and the National Guard Bureau, the National Guard team. I complement them. They just established and released a cyber strategy, for example, just last month, as a matter of fact. And we were part of that dialogue about, so how do we make sure we're doing, you know, an integrated approach within the DOD here? This can't be an Active-only component or civilian-only component.

As you and I have previously discussed the aspects of your question, in some ways, you know, we're beyond, you know, my immediate responsibilities. What I've tried to work with the National Guard Bureau is, so how do we create a structure that enables us to access the full range of capability? Not just units, but, to your point, Hey, how do you get down to the individual bubble?

It's similar, in many ways -- putting on my other hat, Director of NSA -- we've tried to do the same thing over time for language. Many people in the Department have language skills that have no connection with whatever their job is that we've trained them to do. And I'm trying to see, Can we do the same thing over time with the Guard and
the Reserve?

Senator Ernst: Certainly. An additional identifier or something --

Admiral Rogers: Right.

Senator Ernst: -- that can be tracked. I think we really need to focus on that much more so than we have done in the past, just because of the continuing threat that we see in cyber out there. And, you know, as -- kind of along this same theme, though, it is such an important part of our national defense, and we're going to have to continue to improve our capabilities and readiness in this area. And so, if you could, in just the couple of minutes that I have left, What more can we do to make sure that we have an adequate pool of really talented individuals that can step up into these fields? We've seen, at large, military recruiting has been very difficult, even for our regular branches of service. So, what can we do to make sure that we are filling the gap with qualified individuals that meet the requirements of today's military?

Admiral Rogers: So, first, to me, you've got to look at it as an ecosystem and realize there's different components to this cyber population, from civilians to Active military to Guard and Reserve. Each one of those components has different attributes. So, one of the things we need to do is come up with solutions that optimize for
each of these subpopulations. So, the Congress, for example, with the Civilian Exemption Service, the CES, effort, that's a big positive for us on the civilian side. On the DOD side, the services are -- for Active, are working through, So, you know, are there other compensation tools, for example, that we can use? Are there other things we need to do in terms of the commitment we make to individuals when they first enlist or get commissioned, in terms of, Can we align them early on and offer them extended service in the cyber arena?

On the Guard and Reserve, it's a similar kind of thing, though one -- it goes to your point -- the one thing I've -- it's been a little while since I had this conversation with General Lengyel, but, outside the Army Guard and the Army Reserve and the National Guard, the other services tend to use Reserves on a cadre status, as opposed to units. And one of the things that I'm trying to work with my Guard teammates on, Is there a way to both use the unit structure that's traditional within the Guard, but also maybe a cadre kind of thing? That gets to your point about, How do we access individual skills? We are clearly not there yet, but I'm wondering, Is that a part of the future structure that we need to be looking at, that we haven't, to date?

Senator Ernst: Right. And thank you. My time is expired, but certainly this is an issue we need to wrangle
with and make sure that we're coming up with an appropriate
answer.

So, thank you, Admiral, very much.

Senator Inhofe: Thank you.

Senator Nelson.

Senator Nelson: Admiral, thank you for your public
service, your long service. And we wish you well in
retirement.

Since Senator Rounds is not here, I will speak for him,
in that we have the privilege of leading the Cyber
Subcommittee. And I want you to know that we think the
public sectors in the Department of Defense are woefully
unprepared and split and segmented and not coordinated to be
able to handle now what is one of the greatest threats to
our national security, the cyberattacks that constantly
come. And we feel that about the private-sector community,
as well.

Now, having said that, Mr. Chairman, I want to enter
into the record a letter that Senator Blumenthal, Senator
Shaheen, and I sent to the Secretary of Defense, February
the 6th. And one of the things that we ask is that the
National Mission Teams, which are part of U.S. Cyber
Command's Cyber Mission Force, should be ordered to prepare
to engage Russian cyber operators and disrupt their
activities as they conduct clandestine influence operations
against our forthcoming elections.

Would you enter that into the record, Mr. --

Senator Inhofe: Without objection.

[The information referred to follows:]

[COMMITTEE INSERT]
Senator Nelson: Now, Admiral, let me ask you. Is there any question in your mind that they have -- they, the Russians --

Admiral Rogers: Russians.

Senator Nelson: -- have conducted these kind of activities against our past election?

Admiral Rogers: No, sir.

Senator Nelson: Okay. And, in an answer to Senator Reed, you had said, "Yes, if the Russians were successful," as if there was some doubt in your mind that they had been successful. That's not the case --

Admiral Rogers: No, sir, I apologize. The point I was trying to make -- the quote that Senator Reed used was from the strategy, where it talked about acts of "significant consequence." And I was trying to get to the "consequence" --

Senator Nelson: Okay. So --

Admiral Rogers: -- piece of the plan.

Senator Nelson: So, we have been attacked, and there are a lot of us that feel like we are still being attacked and that we're going to be attacked, particularly with regard to our elections, which we consider as critical infrastructure. And let the record note that you nodded affirmatively. So, what's the holdup?

Admiral Rogers: Well, I'd say there's a series of --
and again, this is much broader than the DOD, much broader
than Cyber Command -- Department of Homeland Security is
overall responsible for this -- the election infrastructure
within the segments that private -- that have been
identified as critical infrastructure. They're the sector
lead. In fact, I've had this conversation with the
Secretary of Homeland Security within the last couple of
weeks about what we're doing to try to generate insights and
knowledge to try to help their effort in their leadership
role.

Senator Nelson: Let me be appropriate and respectful
--

Admiral Rogers: What?

Senator Nelson: -- but let me interject, please,
because time is fleeting.

Admiral Rogers: Sir.

Senator Nelson: Let's get -- so, for someone who is
looking out for the common defense of this country to say,
"Well, they've got the lead, and this is that, but I'm the
Cyber Commander, and it's going to be a combatant command"
-- that doesn't cut it over here.

Admiral Rogers: Yes, sir. The challenge for us is, we
have this thing called the law and the legal framework that,
right now, shapes what DOD can and cannot do.

Senator Nelson: So --
Admiral Rogers: I'm not trying to minimize that. It

Senator Nelson: -- what do you need --

Admiral Rogers: -- certainly impacts me --

Senator Nelson: -- Admiral --

Admiral Rogers: -- as an operational commander.

Senator Nelson: -- what do you need, as the commander, to say, "Go after and punish these guys that are trying to tear apart our critical infrastructure"? What do you need?

Admiral Rogers: So, I'd need a policy decision that indicates that there is specific direction to do that. And then I would need -- again, I'd have to tee up -- the normal way we work this process, I would then be tasked to tee up some specific options. And I'd rather not go into the specifics of any of that. And they would be reviewed by the Secretary, the chain of command. The Secretary ultimately would make a recommendation to the President as what he, the Secretary's, views are here, and then, based on that, we'd be given specific direction, potentially, and specific authority.

Senator Nelson: So, you need a direction and specific authority from the White House.

Admiral Rogers: Right. The President ultimately would make this decision --

Senator Nelson: From the President.
Admiral Rogers: -- you know, in accordance with a recommendation, in my experience, from the Secretary of Defense. And others. I would assume the Department of Homeland Security and others would be --

Senator Nelson: So, the chain of command --

Admiral Rogers: Yes, sir.

Senator Nelson: -- is what you need.

Admiral Rogers: Sir.

Senator Nelson: All right.

Let the record reflect that we have written to the Secretary of Defense, February the 6th, and would appreciate an answer.

Thank you, Mr. Chairman.

Senator Inhofe: Thank you.

Senator Perdue.

Senator Perdue: Thank you, Mr. Chairman.

And, Admiral, thank you for your --

Admiral Rogers: Sir.

Senator Perdue: -- decades of service. I remember your testimony last year. You've been nothing but consistent, talking about speed and agility. I hope, in retirement, you'll find a way to continue to nudge us toward that goal.

I've got a question to follow up on a couple of questions we've already had today. And recently the Defense
Science Board -- last year, actually -- concluded -- and there's a quote here, "For at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States ability to defend key critical infrastructures." Sir, do you agree with that conclusion?

Admiral Rogers: I mean, we were a part of that effort with the DSB. There is no doubt that, for right now, I would argue, technology favors the offense vice the defense. I mean, just what you're -- the scope of what you're trying to defend, the scope of potential vulnerabilities or -- boy, it keeps you awake at night.

Senator Perdue: So, the ability to preclude it is minimal. And you mentioned, last year --

Admiral Rogers: Well, "preclude it," from a technical standpoint.

Senator Perdue: Yes.

Admiral Rogers: But, then that gets into the whole broader question about, Are there other activities that could be brought to bear that would convince --

Senator Perdue: Well, that's my next question --

Admiral Rogers: -- you know, on --

Senator Perdue: -- is deterrence.

Admiral Rogers: Yes, sir.

Senator Perdue: You talked, last year, about
1 deterrence. And so, has our ability to deter these types of activities -- you know, a nuclear attack, we deter by having the threat of mutual annihilation, right? So, in the cyber space, what is our deterrence capability today, relative to where we were a year ago? And is it adequate to defend against intrusion?

And I want to add to that, specifically, with -- we've had these questions about election. In your mind, are we capable -- the United States -- of defending our election, this coming year?

Admiral Rogers: Now, I'm not an expert on the electoral system, as a whole. I haven't personally looked at it as a target, so to speak, and asked myself --

Senator Perdue: But, that -- doesn't that speak to the issue? I mean, I know Homeland Security is charged with that.

Admiral Rogers: Right.

Senator Perdue: But, is their capability up to your capability, in Defense? And then you get inside DOD, you've got -- each service has their own growing capabilities. So, the question I have -- and we've all talked around it here -- is, So who's really in charge of getting the highest and best deterrence, detection, and preclusion capabilities regarding, let's just say, an election, as one part of our"
Admiral Rogers: So, in our constitutional structure, States largely have overall responsibility for the execution of an election process. Within the Federal Government, the Department of Homeland Security is overall responsible for providing government resources to assist the States in the execution and defense of that structure. Again, that is a DHS lead role. So, I don't -- in my role as Cyber Command, I'd be the first to admit, I'm not talking to individual State officials about, "Walk me through what your structure is, give me your assessment of where you think you are." I'm trying to generate insights and knowledge now that help inform this with a readiness to -- if directed, to potentially do more.

Senator Perdue: You interact with DHS --

Admiral Rogers: Oh, yes, sir.

Senator Perdue: Okay.

Second thing, following up on the deterrence capability. What are the menu of options that you, in the Department of Defense, can give the President, should he so choose to respond to the cyberattacks, if we -- if we have a deterrent, then the question is, Is there a like response, similar response? And what are the menus -- what's included in the menu for the President?

Admiral Rogers: So, the first point I would make is, number one, merely because someone comes at us in cyber
doesn't mean we should automatically default to a, "We have just to respond in kind." I have always urged, We need to think more broadly, look at the full range of levers and capabilities, as a Nation, that we --

Senator Perdue: Have we ever responded in kind?

Admiral Rogers: Oh, there are certain specific steps that have been taken over the course of the last couple of years. Again, to have an argument about -- Is it sufficient or not? But, there have been some specific steps taken.

And again --

Senator Perdue: Well --

Admiral Rogers: -- I would rather not get into that --

Senator Perdue: I understand that, and I wouldn't ask that in open --

Admiral Rogers: -- publicly.

Senator Perdue: -- an open hearing. But, it's pretty obvious to me, as one Senator sitting here, that the diplomatic efforts here are failing, that the activity is really one-sided --

Admiral Rogers: Right. We're not where we need to be, or where we want to be. I don't think there should be any --

Senator Perdue: No, and I want to -- I now want to about, What can we do about it? And that is -- go back to speed and agility. We're going to be about 1.8 million
cyberwarriors short over the next 5 years. There's a --

Admiral Rogers: As a nation --

Senator Perdue: -- as a country, both -- in all three

of these -- FBI, DHS --

Admiral Rogers: Right.

Senator Perdue: -- and DOD. So, the question is --

we're not going to win that war against China, for example, in terms of the ability to put cyberwarriors in the field.

The question is, Where does -- where do technology and, like, artificial intelligence come to bear? And where are we climbing that hill, in terms of -- if this were a trigger puller, we'd stand up a number of soldiers against their soldiers, and all that. That's a historical -- that's the --

Admiral Rogers: Right.

Senator Perdue: -- the last war. The future war may be, you know, how to -- who's got the best minds focused on artificial intelligence, robotics, et cetera, et cetera?

Just on this specific case, where are we, in terms of artificial intelligence? And how is that going to help us face the shortfall in cyberwarriors over the next 5 years?

Admiral Rogers: So, we're clearly looking at, What are the technical applications and capabilities out there that enable us to optimize the human capital piece of this, that are also -- I'm also interested in the fact guys as -- to
your point, we are not going to Industrial Age our way out of this --

Senator Perdue:  Right.

Admiral Rogers:  -- with, Well, it's just hire 10,000 more people.

Senator Perdue:  Right.

Admiral Rogers:  That's not going to get us --

Senator Perdue:  Right.

Admiral Rogers:  -- where we need to be.  And that's not a sustainable strategy. Therefore, among the things we're looking at -- and we're not the only ones -- so, How can you apply technology to help overcome the human capital piece?

The other point I would make is, again, don't just focus on cyber versus cyber. How do we bring this broader range of capabilities in place to convince actors out there -- nation-states, criminals, nonstate actors -- "You don't want to engage in this behavior, either because you're not going to succeed or because, quite frankly, even if you do succeed, the price you will pay will far exceed any benefit you might gain"?

Senator Perdue:  Yeah.

Admiral Rogers:  That's where we've got to get to.


Thank you, Mr. Chairman.
Senator Inhofe: Senator Shaheen.

Senator Shaheen: Thank you, Mr. Chairman.

And, Admiral Rogers, thank you for your service. We will miss you when you retire.

I want to follow up on both Senators Reed and Nelson's questions about the 2016 election and the action of the administration. I just want to be clear. As I understand, you said that President Trump has never ordered CYBERCOM to take any action to defend or thwart Russian attempts to meddle in the elections this fall. Is that correct?

Admiral Rogers: So, I said I've never given -- I've never been given any specific direction to take additional steps outside my authority. And I have taken the steps within my authority, you know, trying to be a good proactive commander. Because my view is --

Senator Shaheen: But, no one from the administration has asked you to take any additional steps. Is that correct?

Admiral Rogers: I haven't been granted any, you know, additional authorities, capacity, capability. No, that's certainly true.

Senator Shaheen: I understand that to be a confirmation of what I just said. Is that correct?

Admiral Rogers: I thought that's what -- I apologize.

Senator Shaheen: Okay.
Admiral Rogers: All right.

Senator Shaheen: It's come to my attention that the Department of Defense contracts with IT companies that share sensitive source code data with Russia and other hostile governments while they do business overseas, and that this practice risks exposing sensitive underlying codes within our national security platforms to hostile governments. And, as I understand, there aren't any safeguards, like disclosures, to protect against these risks. Can you confirm whether that's the case and what the role of CYBERCOM is in ensuring the safety and integrity of DOD's platforms?

Admiral Rogers: Right. So, first, I have no -- Cyber Command has no direct role with non-DODIN -- with civilian users here, if you will. Now, having said that, I'm aware of this issue, and we have worked with others in the Department to try to address, "Okay, so what are some of our key vendors and providers doing, here?" There have been several incidents where I've actually bore -- dug into execution-level, "Walk me through exactly what you've done with your code. Walk me through exactly who had access to it. I want to compare this version that you tell me you shared with them versus what we currently are using within the DOD." I've done that in a couple of instances.

But, your point goes to -- and several of you have
raised it already -- going to a broader dialogue about, What should the nature of the relationship be between the Department and its key infrastructure in this digital world that we're living in? And it just forces us to step back and look at things very differently, to me. We never used to think about things, 10 years ago, about, "Who are you sharing source code with? You know, who are you doing your testing with?" In the world we're living in now, those are the kinds of discussions that we've got to have. "Who are your supply-chain providers?"

Senator Shaheen: So, who has the responsibility to decide that? If it's not CYBERCOM, is it the Secretary of Defense?

Admiral Rogers: So, the Defense Security Service has overall responsibility within the DOD for the interaction with our cleared defense contractors from a cybersecurity perspective. And I will partner with DSS. The FBI is also involved here. One of the discussions that currently I'm raising within the Department is -- experience teaches us, I think, we need to step back and ask ourselves, Do we have this model optimized? And I won't go into the specifics, but there's a specific scenario we're working our way through right now that I'm trying to use as an example of: This is why we need to make some fundamental change. And I'm glad to talk about that in a closed --
Senator Shaheen: So, should CYBERCOM have that responsibility, or should someone else have it?

Admiral Rogers: I don't know. Part -- quite frankly, one of my challenges, you just look at the things we've talked about in the last 40 minutes, where you have said to me, "Hey, why doesn't Cyber Command to do this? Why doesn't Cyber" -- and I'm going -- the challenge for us is about prioritization, aligning mission with resources, and trying to figure out what's our role with a broader set of partners? And so, one of the points I try to make within the DOD is, "Be leery about viewing Cyber Command as the end-all/be-all for everything." If we try to do everything, we're going to suboptimize ourselves, so we need to focus on one of the priority areas.

Senator Shaheen: And that makes sense to me, but the concern I have is, Who's in charge? And, unless there's somebody who's responsible for coordinating activities for dealing with what Homeland is doing and what Cyber Command is doing and what DOD is doing and what the White House is doing, nobody's going to be in charge. And --

Admiral Rogers: Yes, ma'am.

Senator Shaheen: And so, it seems to me that that's a challenge that we have right now. And, as you look at what our both defensive and offensive strategy is around cyber for the United States, do you believe that we have those --
that strategy in place? And could you articulate that, either now or in a closed --

Admiral Rogers: I mean, I believe --

Senator Shaheen: -- in a way that we can understand?

Admiral Rogers: -- I believe we have a structure in place, with well-defined responsibilities, but, as we said previously, my argument would be, I think experience is showing us that we need to be mindful -- while we understand that structure, is it generating the outcomes that we want? And my answer would be, We're not where we need to be. So, that would argue, doing more of the same is not necessarily going to generate different outcomes. Even as I acknowledge I have a narrowly defined role, but I try to, along with others, act as a, "Look, we need to focus on this area."

Senator Shaheen: Well, I would certainly agree. I don't think a structure and a strategy are the same thing. And, while we may have a structure in place, it doesn't seem to have produced a strategy that's easily understandable.

Admiral Rogers: Ma'am.

Senator Shaheen: Thank you.

Thank you, Mr. Chairman. That's a statement. I'm not asking for a response.

Senator Inhofe: Senator Fischer.

Senator Fischer: Thank you, Mr. Chairman.

Good morning, Admiral. It's nice to see you.
Admiral Rogers: Ma'am.

Senator Fischer: Admiral, the NDS highlights Cyber's importance, I think, quite a bit. And how does that National Defense Strategy's prioritization of long-term strategic competitions with Russia and China impact CYBERCOM's mission?

Admiral Rogers: So, I like the fact that the strategy expressly calls out cyber as a domain. The strategy also expressly calls out the fact that we've got peer competitors and near-peer competitors in here that we have -- within the cyber arena, that we have to be capable of dealing with. I also like the fact that the strategy specifically calls out competition -- trying to remember the phrase -- it's "competition below conflict" -- at a level below conflict, you know, the so-called gray area -- which I think is very powerful. That gray area goes to many -- much of the discussion we've had so far this morning. This activity that is occurring, short of armed conflict, if you will, that is generating strategic advantage for others and not in our best interests. I like the fact that the strategy acknowledges we are living in a world where this is now becoming the norm, and we have got to figure out how we're going to deal with this.

Senator Fischer: And, as we look at that continuing focus with our peer competitors -- with Russia and China --
I think that means we're going to have to do more with less, and we may see less of a focus on other areas, where, in the past, CYBERCOM's been very focused, whether it's with the global terrorists or with Iran and their proxies. So, with those tradeoffs, I think that brings a lot of risk. How do you propose that CYBERCOM and the Department are able to handle that type of risk?

Admiral Rogers: So, within the last year, I and others made an argument, and the Secretary bought off on it, where I said, "Look, we need to increasingly treat Cyber Command as a high-demand, low-density resource, where we have to acknowledge there's not enough capacity to do everything we want." So, we need a prioritization of a risk-based model about how we're going to allocate our capabilities. And we've got to continually reassess this, just like we do with ballistic missile defense, with ISR, with SOF forces. We shouldn't be viewed any differently.

And so, we put a new process in place. I just made an argument, and was granted authority, to reallocate some of our capability against some of the challenges you've already talked to me about within the last 40 minutes or so. That didn't exist -- a year ago, that process didn't exist. It wasn't envisioned. The thought was the cyber forces that we had created would be permanently aligned. I argue that's not just going to -- there's just not enough. It's not
going to get us where we need to be.

Senator Fischer: Do you see that increased focus on a high-end fight -- is that primarily going to impact the training, or is it going to impact operations?

Admiral Rogers: It's probably a combination of both. I don't necessarily view it as a binary --

Senator Fischer: Either/or.

Admiral Rogers: -- one or the other. The positive side -- you know, as I said, I've been in command almost 4 years. In those 4 years, I haven't run into a situation where we didn't have some level of capacity and expertise -- or some level of capability or expertise. The challenge is capacity. It's, "Okay, I can deal with this in a reasonable level of places, but if I get into something larger, that becomes a challenge."

Now, no one should think for one minute -- I am proud of the capability Cyber Command has, and I am confident in our readiness to execute our mission, even as I acknowledge that there's challenges.

Senator Fischer: Okay. When you -- when you're talking about capacity, you're building a 6200-strong Cyber --

Admiral Rogers: Right.


Admiral Rogers: Sir.
Senator Fischer: How adequate do you believe that force is going to be compared to the threat that we're seeing today?

Admiral Rogers: So, that was based on an assessment -- boy, it's almost 10 years ago now, when we did the groundwork about, What do we think the structure --

Senator Fischer: But, that hasn't really changed.

Admiral Rogers: No. So, what we said was, Let's build the force out. So, as I said, we'll complete the buildout by the end of the fiscal year. The argument I'm trying to make now is, So based on the 8 years of actual runtime, that suggests to me that the way that we've structured some of the teams, I would like to change. And I told the services, "I will leave this alone until you complete the mission generation." But, what that -- once that's done, I'd like to retool this a little bit, because I think we can take advantage of the lessons of the last 8 years. I think it also argues, we're probably going to need some level of additional capacity over time. And that's something I'll be talking to my successor about. I think that's going to be a key thing for him during his time as -- in command.

Senator Fischer: It seems like we -- we hear this over and over again, a lot of the same challenges. And I realize the NDS is out now, and it's presenting us with a strategy. But, it's frustrating sometimes, on our side, that --
1 don't know if we're seeing much progress.
2 A last question for you. I was a little confused by an
3 earlier statement, so I wanted to clarify that. You have
4 testified, in the past, that you do not support creating a
5 special corps or service focused on cyber.
6 Admiral Rogers: Yes, ma'am, that's true.
7 Senator Fischer: Okay. Thank you very much.
8 Senator Inhofe: Thank you.
9 Senator Blumenthal.
10 Senator Blumenthal: Thank you, Mr. Chairman.
11 Admiral, thank you for your service. We will miss you,
12 as others have said.
13 Have you read the Special Counsel's indictment against
14 13 Russians and several Russian entities?
15 Admiral Rogers: I haven't read the actual indictment.
16 I've seen the media reporting on it. I haven't seen the
17 actual indictment.
18 Senator Blumenthal: Well, I recommend that you do so,
19 sir, with all due respect. For us, as Americans, it is an
20 incredibly chilling, absolutely terrifying account of an
21 attack on our democracy. You refer to it as a series of
22 actions that, quote, "threaten the foundations of our
23 democracy." I think that's a very polite way of putting
24 this act of warfare. In fact, the Russians themselves refer
25 to it as informational --
Admiral Rogers: Informational.

Senator Blumenthal: -- warfare. That's from them, not from us. And so, I feel a sense of urgency about this ongoing warfare against our democracy that I feel, so far, is not reflected in the response from our Department of Defense. That's one of the reasons why Senators Nelson and Shaheen and I wrote to the Secretary of Defense last week and asked for engagement of Russian cyber operators and disruption of their activities. And I understand from you that your feeling is, you have not been given authority to take additional action. That's correct.

Admiral Rogers: Sir.

Senator Blumenthal: Have you asked for that authority?

Admiral Rogers: No, I have not. I've tried to act within the authority that has been granted to me to be aggressive.

Senator Blumenthal: Why have you not asked for additional authority?

Admiral Rogers: Because I guess my sense right now is, I'm not sure that the capabilities that I have would be the optimal or only response to this. I think we need to --

Senator Blumenthal: It may not be the only response --

Admiral Rogers: If I could -- I apologize.

Senator Blumenthal: -- but wouldn't you agree that it is a necessary response?
Admiral Rogers: It could be a part of a response. I would certainly acknowledge that. I just think we need to step back and look at this very broadly. Because one of the arguments, not just the -- this current piece, but others -- is, "Be mindful of falling in the trap that, just because someone comes at us in cyber, that we have to default to immediately going back and doing the exact same thing." I -- and just have -- I've always believed we need to step back and think a little bit more broadly about it, and just don't default. It's because of that, you know, that I have not done that, to date.

Senator Blumenthal: Well, for how long, with all due respect, are we going to step back and look broadly at this ongoing attack? I mean, literally last week, in the wake of the Parkland shooting, the bots, the fake accounts, again and again, disrupting, sowing discord, continuing to attack our democracy in ways that most Americans should find absolutely intolerable, may I suggest that seeking that additional authority perhaps is appropriate at this point?

Admiral Rogers: Sir. Again, much of what you're asking me -- I'm an operational commander, not a policymaker. That's the challenge for me as a military commander.

Senator Blumenthal: Wouldn't you agree with me that the President himself is aware of these attacks and should
give you that additional authority?

Admiral Rogers: I think the President is certainly aware. Sir, I am not going to tell the President what he should or should not do. I'll use my chain of command to make my recommendations to the Secretary as to, "Hey, sir, hey, within the DOD mission set and within the responsibilities that you have allocated to the Cyber Command, here's what I think we can and should do."

Senator Blumenthal: Well, without belaboring this point, would you agree with me that the Russians have been in no way deterred from --

Admiral Rogers: Oh, yes, sir, I think that's true.

Senator Blumenthal: They're doing it with impunity. They could care less what we think. They're continuing to attack us.

Admiral Rogers: Yes, sir.

Senator Blumenthal: So, thus far, the response of the United States of America to this ongoing attack has been completely inadequate to --

Admiral Rogers: It hasn't changed the calculus, is my sense. It has not --

Senator Blumenthal: It has not changed the calculus --

Admiral Rogers: -- changed the calculus or the behavior on the part of the Russians.

Senator Blumenthal: And it hasn't changed their
behavior.

Admiral Rogers: Right, that's my sense.

Senator Blumenthal: And they have paid no price for meddling in 2016 election or --

Admiral Rogers: They haven't paid a price at least that's sufficient to get them to change their behavior.

Senator Blumenthal: Well, they haven't paid any price, so far as I can see, have they?

Admiral Rogers: You could argue some of the sanctions that were -- that have been imposed -- you could also argue some of the indictments -- again, I don't think it's fair to say nothing has been done, although, again, you're getting way outside my lane as an operational commander, sir.

Senator Blumenthal: But, it has been completely inadequate so far.

Admiral Rogers: It certainly hasn't generated a change in behavior that I think we all know we need.

Senator Blumenthal: Thank you, Mr. Chairman.

Senator Inhofe: Senator Hirono.

Senator Hirono: Thank you, Mr. Chairman.

Admiral Rogers, I do join my colleagues in thanking you for your service, not only in Cyber Command, but also your 37 years of service in the military.

You have been asked a number of questions about the Russian interference with our elections and questions about
who's in charge. And you testified that Department of
Homeland Security is the sector lead on combating Russia's
-- countering Russia's efforts to tamper with our elections.
Now, it seems, to me anyway, that perhaps Cyber Command has
the best resources and best equipped to actually do
something in this area. You are the operational person.
But, you don't have specific authority from the President or
the -- or anyone else, for that matter, to go forward. Now,
you did also indicate that you are -- I believe you used the
word "constant contact" with Department --

Admiral Rogers: I said "regular." I said --

Senator Hirono: Regular.

Admiral Rogers: -- I interacted with them --

Senator Hirono: Regular --

Admiral Rogers: -- regularly.

Senator Hirono: -- contact with Department of Homeland
Security. And the sense that we have -- I have -- is that
the -- that I wonder what the Department of Homeland
Security, which is charged with countering the Russian
interference with our elections -- what they are doing. So,
since you are in regular contact with Homeland Security,
what have you advised DHS to do in this area to counter
Russia's interference with our election --

Admiral Rogers: What have I advised DHS to do in the
execution of DHS's mission? That's not really --
Senator Hirono: Yes. Have you given them any advice?
Admiral Rogers: That's not really my role, ma'am.
Senator Hirono: No, but you are in constant contact.

What are you in constant --
Admiral Rogers: So, we talk about --
Senator Hirono: -- regular contact about?
Admiral Rogers: -- "Tell me what you're doing. Tell me how you're organized. What are the capabilities that Cyber Command, for example, could support you with?" Those are the kinds of discussions. I also make sure the information flow, "Are you getting the benefit of the insights that we're generating" --

Senator Hirono: So --
Admiral Rogers: -- "based on actions that we have taken?"
Senator Hirono: So --
Admiral Rogers: Those are the kinds of --
Senator Hirono: -- with regard to those kinds of conversations, then is Homeland Security doing what they need to be doing to counter Russian interference, continuing interference with our elections?
Admiral Rogers: You need to talk to them, ma'am. I don't have full knowledge of everything the Department of Homeland Security is doing here. Therefore, it would be --
Senator Hirono: Yes, I understand that.
Admiral Rogers: -- it would be an ill-formed opinion

--

Senator Hirono: I get that.

Admiral Rogers: -- on my part to assess their

performance.

Senator Hirono: So, I'm trying to get at -- with all
the resources and the awareness that you have, what kind of
specific advice you have given to Homeland Security, because
we do not get the impression that they are doing what's
adequate to -- definitely to counter anything that the
Russians are doing, certainly not to the point where they
will stop doing it.

Admiral Rogers: Right.

Senator Hirono: So, I hope that, at some point, in
some other committee or in this committee, we'll be able to
ask those kinds of questions of the Homeland Security
Secretary, because what they're doing to -- with our
elections does have an impact on national security. And, as
you say, they are seeking to undermine our institutions.

I would also like to join Senator Ernst in her focus on
the Department of Defense fully utilizing the cyber
capabilities of our Reserves and National Guard. That's
just a statement. And I think you concur with that.

As you leave your command, I am wondering, What would
be your suggestion that your successor, you know, focus on
as he or she -- it'll probably be a he -- take over Cyber
Command? What are the things that you would want the new
person to focus on?

Admiral Rogers: So, "You're in" -- this is what I
would say to the individual, assuming the nominee is
confirmed, "You're inheriting a structure that reflects
choices we made 8 to 10 years ago. We need to step back and
ask ourselves, Is the structure optimized for today and
tomorrow? And how do we take the lessons of the last 8
years, where we've done a whole lot of activity on the
defense, in the offense, working with the private sector?
There are insights there that I think we can harness to look
at, How do we evolve the structure?" I'd also argue, we
need to step back -- and you have raised this with me
already this morning -- how do we better work the DOD role
and the defense industrial base and the cleared defense
contractors? We've got to get a different dynamic here.
We've got to look at that differently. And then, more
broadly, Cyber Command -- and again, it goes to some of the
points you've raised -- Cyber Command, in its role,
partnering with others, how do we do this in a much more
integrated way? That'll be something that I hope maybe I
can continue to provide opinions on in my next life.

Senator Hirono: Yes, how to get an integrated
structure for speed and agility. So, you have different
departments: DHS, FBI, Treasury. Who should take the lead in creating this integrated structure?

Admiral Rogers: Well, that's, you know, clearly the role of the administration within the executive branch. That's their task. And I know they're working their way -- again, DOD, we're going to support this. There's an ongoing review right now on this same question. So, we'll see what comes out of that.

Senator Hirono: Is there something that Congress can do to enable one entity, one of these agencies, to take the lead in integrating our structure?

Admiral Rogers: I'd -- you know, I'd prefer to give the executive branch a chance to say, "So, tell me what you think the plan is." Now, I -- I'm not trying to minimize the role of the Congress. Please, Senator, that's not what I'm trying to say.

Senator Hirono: Thank you.

Thank you, Mr. Chairman.

Senator Inhofe: Senator Heinrich.

Senator Heinrich: Thank you, Mr. Chairman.

Admiral Rogers, this committee has long expressed concern about the lack of an effective doctrine to help deter cyberattacks before they happen. The FY18 NDAA specifically directed the development of a national cyber doctrine. Why don't we have one yet? We've been talking
about this for years.

Admiral Rogers: Right. So, I don't want to speak for others. I flatout can't tell you why. The point I'm trying to make, as the Commander, is, "Hey, we need this," that there would be value, not just for Cyber Command, not just for the Department of Defense, but for the Nation as a whole. As I've said, there is an ongoing effort right now. I hope this is going to generate some of the points that you make. I think it's frustrating to all of us. It's not because of willful ignorance or neglect or negligence, but we clearly haven't put ourselves where we need to be.

Senator Heinrich: Is it even possible to achieve cyber deterrence when we don't have some sort of public-facing articulated cyber doctrine that gives our enemies pause?

Admiral Rogers: Well, I think deterrence has multiple components, from capabilities to a sense of, you know, what we can and can't do, and what we will and won't do. So, I would also argue, Let's not think of what --

Senator Heinrich: So we have some inherent deterrent --

Admiral Rogers: Right.

Senator Heinrich: -- value in our capabilities.

Admiral Rogers: Yes, sir.

Senator Heinrich: If we had an articulated doctrine --

Admiral Rogers: That would also help --
Senator Heinrich: -- that drew some -- you know, that pointed out that there would be consequences, would that increase our deterrent ability?

Admiral Rogers: I think that would increase it, but I also -- the -- I apologize -- the other point I wanted to try to make was, But don't think a strategy, in and of itself, is the panacea. I think --

Senator Heinrich: Sure.

Admiral Rogers: -- it's an important --

Senator Heinrich: Yeah.

Admiral Rogers: -- component of where we --

Senator Heinrich: Absolutely.

Admiral Rogers: -- where we need --

Senator Heinrich: We need tools.

Admiral Rogers: -- to be, but it's the tools and the underpinning, as well. Once you get that framework, then it's, So what do you do to actually get to actionable outcomes?

Senator Heinrich: So, right now, as my colleagues pointed out, the Russian state continues to use bots, they continue to --

Admiral Rogers: Right.

Senator Heinrich: -- use trolls and other, basically, information warfare tools to sow division in this country --

Admiral Rogers: Yes, sir.
Senator Heinrich: -- to sow doubt. Has our response been adequate to create any sort of visible deterrence to those activities?

Admiral Rogers: It clearly has not changed their calculus. It's not changing their behavior.

Senator Heinrich: I think that draws just sort of a fine point on -- we need to be doing everything we can right now to increase that deterrent value, because it's not being effective.

Let's take a hypothetical for a moment. Tomorrow, there's a nation-state cyberattack against our power and energy sector. It results in power outages, it results in oil and gas pipelines shutting down. Take a moment and assume that the other decisionmakers, folks at DHS as well as the administration, are in agreement that this is a hostile nation-state attack, and who it's coming from. The White House wants to respond in the cyberdomain immediately.

Without talking about what that looks like, are you ready?

Admiral Rogers: It -- there are so many variables in what you -- so, who's the actor? What kind of capability was used? What specifically are we looking to defeat or overcome? It's one of those -- I apologize --

Senator Heinrich: Are you confident in your tools and your team to be able to respond immediately?

Admiral Rogers: It -- the tools are optimized for
specific actors and specific -- and again, I apologize, I
don't want to get into the specifics of --
Senator Heinrich: I don't want to give you specific
actors, but you know --
Admiral Rogers: Right. But, the capabilities are
optimized for specific actors and specific configurations,
in many ways. So, there are so many variables -- the other
thing in all this is, you know, time. It's one of the
reasons why I think we've got to get a much more integrated
day-to-day approach to this. Because one of my challenges
is: Look, my experience as a military commander teaches me,
doing discovery learning while I'm moving to contact -- I'm
being told, "Hey, I want you to forestall the following
adversary." If the first time I've dealt with this
potential adversary is in the scenario you've outlined, then
I'm doing a lot of discovery learning as I'm going to
contact. That's --
Senator Heinrich: Let's make --
Admiral Rogers: -- not optimal.
Senator Heinrich: -- the assumption that it's somebody
we've been planning for for a --
Admiral Rogers: Right.
Senator Heinrich: -- long time.
Admiral Rogers: Then that's a little different
scenario. And again, it depends on the --
Senator Heinrich: You mentioned --
Admiral Rogers: -- specifics, but --
Senator Heinrich: -- a few in your --
Admiral Rogers: Yes, sir.
Senator Heinrich: -- initial testimony.
Admiral Rogers: That there are capabilities for us.
Senator Heinrich: Okay.

You have talked for years about, sort of, your top three cyber concerns: critical infrastructure, data manipulation, and attacks from nonstate actors. Just quickly, compare how you think we're doing on those three, versus how you viewed them, from a risk point of view, when you first took this job. How has it changed?

Admiral Rogers: So, first, critical infrastructure. There's greater recognition of the problem set, which is good. I'm not spending a lot of time, now, saying, "Hey, this is something we need to be focused on." But, I would still argue it's uneven. Some segments, very advanced, doing some great work. Other segments, not so much.

The second area was -- I apologize -- was data manipulation. My argument would -- "Boy, are you watching that unfold now in the world around us?" It goes to the influence piece. I would argue that has gotten worse, because now you've got a major actor, and they're not the only ones, in the form of the Russians, who -- now it's a
conscious part of their strategy, and they're doing it on a regular basis. So, there I would argue we've gotten worse. And the third was --

Senator Heinrich: Nonstate actors.

Admiral Rogers: -- nonstate actors. That one, that surprised me a little bit, in the sense that, while I've -- and I'm not talking criminal, because I would argue criminal activity is still the greatest single segment of activity, from a threat basis, within the cyberspace arena. That has not taken off quite as much as I thought it would, to be honest.

Senator Heinrich: I'm over my time. I apologize, Mr. Chair.

Senator Inhofe: Senator Kaine.

Senator Kaine: Thank you, Mr. Chair.

And, Admiral Rogers, thank you so much for your service and your multiple appearances here.

I was interested that, in the aftermath of the announcements by Director Mueller of indictments of 13 Russian individuals, two Fridays ago, that the President tweeted out -- and I'm just going to use his words; I normally wouldn't use these words, but -- and I'm going to quote him. He said Russia is, quote, "laughing their asses off." And he also said, quote, that "Russia has succeeded beyond their wildest dreams."
I think this is going to be chapter in our life where we're going to just have to acknowledge we've been humiliated as a country. Our democracy has been humiliated. We've had our pocket picked. We've lost what may be, you know, the first real cyber war that our Nation has been in.

You can characterize it a lot of different ways, but I think it's going to be characterized as a chapter of failure. The U.S. Government failed to protect the U.S. democracy.

And I want to ask you, based on your lengthy experience in this position, but really your lengthy experience in service to the country, Where is the source of that failure? Was the failure a failure of imagination? Was it a failure of will? Was it a failure of policy? Was it a failure of structure? Was it a failure of personnel? Was it a failure of leadership? Was it a failure of investment? Was it more than one of those things? We can learn from failure, and we should, so that we --

Admiral Rogers: Right.

Senator Kaine: -- can improve. But, I think the history of this, especially the 2016 election, which has now led to 19 indictments or guilty pleas by individuals, and another three indictments or pleas by entities. It's going to be viewed as a chapter where the U.S. Government failed the U.S. democracy. And I want your best professional judgment, in what may be your last appearance before the
committee in this particular role, as where the source of that failure is, so that we can fix it.

Admiral Rogers: So, I don't think there's one single source of failure, but I'll share some thoughts with you.

So, first, one of the things that's always struck me is, we -- if you go back several years, we tended to define "critical infrastructure" from a very Industrial Age approach. Hey, does it produce a product or service, an outcome? So, for example, using that methodology, we didn't say to ourselves, our electoral process is a critical infrastructure product. Because we're thinking, there's no product or service, so to speak, that it tangibly generates. I mean, there's votes and outcomes. So, the first thing I was struck by is, we need to rethink, What does critical infrastructure really mean to us in this Digital Age that we're living in?

Secondly, I think -- you know, I -- again, I've been in the job for a while. I've been in that part of multiple administrations. I think the thought initially was, We'll go to them, we'll tell them we have awareness of what we're doing, and this will convince them -- and we'll take some initial steps, and we'll convince them that they should stop.

Senator Kaine: Underestimating an adversary.

Admiral Rogers: Right. And that clearly has not
happened. I don't think we anticipated how -- what level of sustained aggressive behavior we were going to see over time, that this wasn't viewed as a one-off, "Hey, it was just about one particular election, one particular outcome," that clearly we're looking at a nation now who views this as a strategic imperative over time for them, that there's value to be achieved in continuing to do this. I don't think we necessarily initially looked at it that way.

And then, the final thing that comes to my mind is -- and it's symptomatic of cyber as a whole -- what do you do when we're dealing with a challenge that crosses so many different lines? So, as I said, in our structure, elections are a State process. Cyber capability -- DOD, DOJ, DH- -- that's the executive -- that's not State, that's a Federal and it's an executive branch. You look at capability in the private sector, how do we -- one of my takeaways is, cyber is going to force us to think outside the traditional lines that we use in assigning -- in defining problems and aligning resources.

Senator Kaine: Let me ask you one more question. I was a mayor and a Governor. Why should mayor -- local officials or State officials today believe that the United States Government will protect the United States democracy in future elections? Because, as I talk to Governors and local officials, they have very grave doubt whether the
Federal Government will act in any way to protect the electoral system from attacks such as those that Russia conducted in 2016. Tell them why they should have confidence that the U.S. Government will --

Admiral Rogers: Well, first, I don't interact with them, but, as a citizen, my attitude would be, "Look, I hope one of your takeaways is, here, while the system is imperfect and clearly has not achieved the outcomes we want, it is not because there aren't motivated, hard-working individuals trying to do things." And that, hopefully, as you've said, you know, we want to be a learning, adaptive nation, here, where we learn and change over time. And that's what I'm hoping we're going to see in the coming months and years ahead of us. Because this is not a, "All we've got to worry about is -- we'll deal with this in 6 months or a year." That's not the way this is going to work, I don't think.

Senator Kaine: Thank you, Mr. Chair.

Senator Inhofe: Senator McCaskill.

Senator McCaskill: I'm going to try to -- I know this ground has gone -- been gone over, but -- first of all, thank you.

Admiral Rogers: Yes, ma'am.

Senator McCaskill: You've been terrific. I'm a big fan of the work you've done.
But, I'm going to try to channel a woman who came up to me at the grocery store not too long ago. She asked me a simple question: "Is Russia at war against our democracy?"

What would you have said to her in the grocery store?

Admiral Rogers: I -- well, a war is, by definition, as a specific legal document aspect to it. And I'm not a lawyer. What I would probably say to her is, "There shouldn't be any doubt we are in a competition with these guys, and they are trying to use every tool they have to gain advantage. And some of that advantage they want to gain is by undermining our very institutions."

Senator McCaskill: That's a lot of words. I said, "Yes."

[Laughter.]

Admiral Rogers: So --

Senator McCaskill: I said, "Yes."

Admiral Rogers: I like to talk to people. I apologize.

Senator McCaskill: I mean, I've just got to tell you, they came after our democracy.

Admiral Rogers: Yes, ma'am.

Senator McCaskill: I can't imagine anything more essential to the United States of America than our democracy. So, the next question she asked me, "Are we strong enough and smart enough that we can keep them from
doing this again?"

Admiral Rogers: Yes.

Senator McCaskill: Okay. So, then the next question she asked me -- I said the same thing -- the next question she asked me, "Are we doing that right now?"

Admiral Rogers: We're taking steps, but we're probably not doing enough.

Senator McCaskill: Okay. So, she wants to know, and I want to know, Why the hell not?

Admiral Rogers: Ma'am, I'm not --

Senator McCaskill: What's it going to take?

Admiral Rogers: I'm an operational commander, ma'am.

You're asking me a question that's so much bigger than me. I don't -- I'm not trying to duck this. I'm trying to say, Here's what my role is. And you're --

Senator McCaskill: It's a problem --

Admiral Rogers: -- asking me something that's --

Senator McCaskill: -- it's a problem, Admiral.

Admiral Rogers: Oh, I don't deny that --

Senator McCaskill: It's a problem.

Admiral Rogers: -- for one minute.

Senator McCaskill: You know, the notion that this country came after the essence of what we are -- the character and value of our country is all about the democracy -- the notion they came after us, brazenly, and
that nobody can sit in that chair and say, "We got this" -- you guys can do this. You give our America's military a mission, and nobody is better.

Admiral Rogers: Right.

Senator McCaskill: The notion that you have not been given this mission to stop this from happening this year is outrageous. It is outrageous. And there's no question that they know we're not coming after them. And, frankly, your response to Senator Reed's question about Cyber Command disrupting their interference, you said, "We have chosen not to engage in the same behavior as Russia." But, defending is not the same behavior as Russia. Preventing and deterring is not the same behavior. They came after us. We're not asking you, "Are you going after them?" We're asking you, "Have you the authority, have you the command to stop them from doing this again to the -- us in 2018?"

Admiral Rogers: I cannot operate out of the DOD information network, ma'am, on a daily basis. I do not have the authority to do that. I don't have the legal authority to defend a State's voting infrastructure --

Senator McCaskill: Well, I'll tell you, Admiral Rogers, if there -- if you don't have the authority to defend our voting structures, then we've -- we've got the ability to fix that. Correct? I believe, Mr. Chairman and Ranking Member, we have the ability to fix the law to give
you the authority to protect our voting systems. Because I
guarantee you, the Secretary of State of Missouri doesn't
have an ability to go after Russia.

Admiral Rogers: Right. Yes, ma'am

Senator McCaskill: I mean, they could harden, but they
can't go after them. The only entity that can go after
Russia is the United States military. That's the only one.

And the fact -- I mean, effectively -- I mean, maybe
Department of Homeland Security can help around the edges,
but their primary mission is not to go after a foreign
nation. It is, in fact, to protect the homeland.

Admiral Rogers: But, again, I would argue, think --
respectfully, think beyond just cyber and responding in
kind. There's a whole -- economic, politi- -- there's a
whole breadth of tools that we could potentially apply here
to try to shape the Russians' behavior and their choices. I
would just urge us, "Don't default to, We've got to go after
them in cyber." I'm not arguing that cyber isn't a
potential part of a broader strategy. I'm not trying to say
that --

Senator McCaskill: I just never thought I'd --

Admiral Rogers: -- for one minute.

Senator McCaskill: -- see the day -- honestly, I never
thought I'd see the day that Russia would go after the heart
of our country.
Admiral Rogers: Ma'am.

Senator McCaskill: Ever. And that we would be sitting here parsing words about whether or not we've got this. I want somebody with your experience and your courage and your tenacity -- I want somebody to sit in that chair and say to the United States of America, "We've got this."

Admiral Rogers: Ma'am.

Senator McCaskill: And until we have that moment, Russia is winning. And that is disgusting.

Admiral Rogers: Yes, ma'am.

Senator McCaskill: Thank you, Mr. Chairman.

Senator Inhofe: Senator King.

Senator King: Thank you, Mr. Chairman.

Guess what question I'm going to ask?

[Laughter.]

Admiral Rogers: Yes, sir. Would this be a Russian -- associated with Russia?

Senator King: It would be. And a deterrence-related question.

Admiral Rogers: Yes, sir.

Senator King: On December 23rd of 2016, the Congress passed the National Defense Authorization Act. In it was a section that required the Secretary of Defense to file a report, on just the questions we've been talking about, within 180 days, which was June of 2017, about the
definition of a "cyberattack," what would be the response.

It talks about operational authorities -- what operational
authority is delegated to the United States Cyber Command
for military cyber operations, how the Law of War applies,
the whole -- a whole list. The purpose of the amendment,
which was in the law, which is in the law, was to establish
a clearly articulated doctrine of response in this kind of
situation. I'm asking you, as an operator, have you been
asked -- have you been tasked with drafting any part of the
response to this requirement, which --

Admiral Rogers: I've been --

Senator King: -- by the way, is now in --

Admiral Rogers: I've been part of the --

Senator King: -- month eight?

Admiral Rogers: -- part of the dialogue about
responding, particularly on the operational piece of this,
in terms of overall responsibility. This is -- the Office
of the Secretary of Defense has the responsibility for --

Senator King: But, I'm asking, Is anybody --

Admiral Rogers: -- replying --

Senator King: -- working on this? We're 8 months in
-- we're 8 months late now.

Admiral Rogers: I apologize. I don't know the
 specifics of the timeline for --

Senator King: But, were you given a deadline, saying,
"We need this by June of" --

Admiral Rogers: I was --

Senator King: -- "2017?"

Admiral Rogers: -- part of this. I don't remember --
I honestly don't remember if we were given a -- can I take
this one as a -- an action to --

Senator King: Yeah, but here's --

Admiral Rogers: -- get back --

Senator King: -- here's what's frustrating, is -- Here
we are, still talking about this issue, when the Congress
made a specific instruction to the Secretary of Defense, and
the President, by the way, was then required to respond to
the Congress within 180 days from that report that should
have been coming in June of 2017, hasn't come. So, you
know, we're way late, and we --

Admiral Rogers: Yes, sir.

Senator King: -- keep talking about this. You and I
have been in probably a dozen or 15 hearings on this, and we
don't seem to be any further ahead than we are -- were
before. And the problem, as you've testified today, and I
think quite accurate and repeatedly, until we have some
clearly articulated doctrine of response to these kind of
attacks, they're going to continue. If all we do is try to
patch our software --

Admiral Rogers: Right.

75
Alderson Court Reporting
Senator King: -- they're going to continue. And you know that, and I know that. What's it going to take? Is it going to take the destruction of the electric grid or the financial system in order for us to finally get to the point of taking this seriously?

Admiral Rogers: Like I said, sir, there is an ongoing -- I'm -- and I'm participating in this. I just -- apologize -- I just don't know the specific timelines here. I'm --

Senator King: Yeah. And I'm not -- I understand you're an operational guy, but you have to understand our -- you're the nearest thing that we have --

Admiral Rogers: I've got it. I know my --

Senator King: You're lucky enough to be here today. But, this is serious business. And --

Admiral Rogers: Yes, sir.

Senator King: And -- well, let me turn to some -- a little more specific question that I think underlines what we're talking about here. What would happen today if you, on your way back to your office, got a call and said the U.S. financial system has been taken down, all the computers on Wall Street are off, the markets are in chaos? I don't mean from a policy point of view. I'm --

Admiral Rogers: No, no.

Senator King: -- talking about --
Admiral Rogers: In terms of --

Senator King: -- what would be the execution? Who's in charge? What would the results be?

Admiral Rogers: So, DHS would have overall responsibility for the provision of Federal support in response to this. My role would be: help to make sure I understand, number one, who was the actor. So, can we identify who did this? Because if I'm going to respond, I have to know who I'm responding to or what I'm responding to. So, one of my first questions, as Cyber Command, would be, Let's make sure we understand what's the characterization of activity, who's the actor, what did they do --

Senator King: Who would take the lead? Who's in charge?

Admiral Rogers: -- how did -- DHS would have overall responsibility.

Senator King: DHS would be in charge?

Admiral Rogers: Sir.

Senator King: Do -- have you -- do you -- have you war-gamed this?

Admiral Rogers: Yes, sir. In fact, I made it a broad reference it -- the finance sector, for example, the scenario you posture here, I've -- we've actually undertaken some very good table tops, specifically, as I reached out to
DHS and the financial sector. And, "Look, we have got to get down execution-level work here, team." So --

Senator King: Well, that's -- and you --

Admiral Rogers: -- we have done --

Senator King: -- repeated talk about integration. And what worries me is that -- whether anyone is in charge. And I guess a followup is, Do we have a serious red-team, war-game process to be sure we're not surprised about how to react when one of these things happens?

Admiral Rogers: I don't know if I'd use the phrase "we have a serious red team." Do I -- is this part of our mission responsibility? Yes. Is this something we train and exercise against? Yes. Is this something we continually assess, looking for indicators of this type of activity before it occurs? Yes.

Senator King: Well, I want to thank you. This may be our last --

Admiral Rogers: Sir.

Senator King: -- time to talk about this. And thank you for your service and your straightforward response, always. And just leave you -- and you know, I hope, as you leave this job, you will leave a memo behind that says, "We are not adequately prepared. We need a doctrine. We need it to be publicly available. We need our adversaries to know that, if they strike us in this realm, they're going to
be struck back." And it may not be cyber. I mean, as you say --

Admiral Rogers: Right. Sir.

Senator King: -- it may be a whole range of things. But, right now, we are not -- we have not done that. And I deeply hope that this is something you can take on as a kind of exit interview.

Admiral Rogers: Sir.

Senator King: Thank you.

Thank you, Mr. Chairman.

Senator Inhofe: Senator Tillis.

Senator Tillis: Thank you, Mr. Chairman.

Admiral Rogers, thank you for being back before the committee.

Could you just give me a brief description, in your tenure in the current role, where you think things have got -- tell me the positive things that have occurred and the things that you wish you had made more progress on in your time in the Command.

Admiral Rogers: So, the positive thing, among the things that jump out at me, it's Cyber's integration with other operational commands, particularly CENTCOM, SOCOM, some things we're doing out in the Pacific with Pacific Command. That has been a real strength. It's something I really -- I knew it was a good day when you have those
commanders publicly talking about what Cyber Command is
doing. And it's not Cyber Command talking about, "Look at
all the great cyber things we're doing. Shouldn't you like
what we're doing?" That's been a real process.

Some of the command-and-control structures -- JTF Ares
that we put in place. How do you build a structure designed
to integrate capability so we can generate effects against
ISIS -- was a slow start, because we were starting from
ground zero, but it has really taken off. That has worked
out very, very well.

The campaign planning in the structure, from a planning
perspective, that we've put in place, particularly that's
been a focus for us over the last calendar year, that -- oh,
that's just some great work. That really sets the
foundation for the future and gets cyber into a much more
traditional, "Hey, look, we're no different in our mission
set than CENTCOM is in what they're -- in terms of the
mechanisms and the framework they're using to plan, or what
European Command is doing." That's a real positive.

If I ask myself, What are the areas where I would --
and the force generation. I mean, we're going to beat the
timeline for FOC. That took a lot of work by a lot of
people. The areas where I -- were not as far along as I
wish we were, tool and capability development and who's
going to do what. We've still got to work this out between,
What's the role of the services and what's the role of the Command? You have give us -- the Congress has given us some acquisition authority. We've started down that road. I think that's a real positive. But, we've got to ask ourselves, So what's the future here?

Senator Tillis: Do we have the timelines on acquisition right with the nature of the developing technology? In other words, are we compressing the time to new capabilities to a point that you feel comfortable?

Admiral Rogers: So, we're -- we're never where we want to be. But, I like the fact that there's been recognition, we need to do this outside the traditional acquisition framework, which was really built to generate these capital-intensive capabilities that take a decade to develop.

That's not our model. That is not what we need. So, I like the recognition of this. It's an area the Secretary's asked me to take a look at over time, so this will be something I'm going to comment on before I leave. I've got some thoughts I want to share on this before I leave.

Senator Tillis: How well have you done on personnel recruiting and retention?

Admiral Rogers: So, if you look at a uniform --

Senator Tillis: As chair of the Personnel Subcommittee, I'm --

Admiral Rogers: Right.
Senator Tillis: -- particularly interested in other 
things that we should be doing as we look at the NDA 
specifically around personnel issues.

Admiral Rogers: So, if you look on the uniform side, 
I'd say we're probably exceeding our expectations. It 
doesn't mean that it's perfect. The biggest challenge for 
me in the 4 years has been less the military uniformed 
component, and the civilian piece is proving to be harder. 
Retention, recruitment -- part of it also now is the 
process. When it comes to the military, we've got a lot of 
people coming to us, many of whom have skills that I can 
apply in cyber. In the cyber world, it's much more about 
going out and trying to find people with the right skills. 
It's a little different dynamic. And so, the civilian piece 
has probably proven to be harder.

Senator Tillis: Well, that's something that we're 
always interested in, in things that we can do to make that 
easier. It's very --

Admiral Rogers: Yes, sir.

Senator Tillis: I can't imagine how you compete with 
the likes of the firm that I worked with on recruiting and 
retaining --

Admiral Rogers: Right.

Senator Tillis: -- some of the top talent. I could go 
and fill the new capability in 3 months that you could take
3 years to do. And I think that we have to continue to look at that. These highly talented people --

Admiral Rogers: Right.

Senator Tillis: -- want an environment where they're moving at the pace of the threat. And that's the last thing.

Since the time you started this role, how would you describe the number and the nature of threats that you're dealing with today versus when you began?

Admiral Rogers: State actors have gotten more aggressive, not less aggressive. The breadth of capability in many states that are of concern to us is growing. You can look at the level of -- I mean, we publicly talk about Russia, China, Iran, North Korea -- you look at the level of investment they are making, it is significant.

Senator Tillis: And how well -- last question -- how good have you gotten at knowing what we don't know? And I've talked about this before --

Admiral Rogers: Right.

Senator Tillis: -- in prior committees, the latent capability. There are a lot of people who express frustration because, when we see malign behavior on the part of, maybe, a state actor or some other organization, the idea is to go out with some sort of a proportionate response in the cyber world. The thing that concerns me with that
is, we really don't know what we don't know about latent capabilities that could ultimately brought -- be brought back to us. Are we at a point where we have any better or more holistic idea of what the latent threats are out there --

Admiral Rogers: I mean, we're --

Senator Tillis: -- in private sector or with --

Admiral Rogers: Right.

Senator Tillis: -- whole of government?

Admiral Rogers: I mean, we're better. But, on the other hand, just as a broad --

Senator Tillis: They're better, too.

Admiral Rogers: Right. Just as a broad operational principle, one of the team -- one of the things I constantly tell our team is, "You must assume we have imperfect knowledge, and we must be capable of acting on imperfect knowledge." So, don't come to me, telling me, "Hey, we think we totally understand." I -- just my experience teaches me, it doesn't always work that way.

Senator Tillis: Well, thank you. And again, encourage you to get any feedback to the committee staff --

Admiral Rogers: Sir.

Senator Tillis: -- in my office on anything that we can do, at least on the recruiting-and-retention piece for any resources going into the NDA.
Admiral Rogers: Yes, sir.

Senator Tillis: Thank you for your service.

Senator Inhofe: Thank you, Senator Tillis.

Let me just make one comment here before going on to Senator Peters.

I was thinking, all during this, less than complimentary comments have been made. I just returned, last night, from 12 -- 13 days in PACOM. Everyone from Admiral Harris, Shaunessy, all the rest of them, I've talked to, all the way around to and including on the DMZ, between South and North Korea. So, all the principals there. I have to say to you -- and this is at PACOM -- they are very complimentary of the work that you've done and the progress that you've made.

Senator Peters.

Senator Peters: Thank you, Mr. Chairman.

And, Admiral Rogers, wonderful to have you --

Admiral Rogers: Senator.

Senator Peters: -- here again. And I'll join in saying thank you for your service. We're going to miss you. It's been great having you before this committee, and I've appreciated your attention to this issue, and personally talking to me about a variety of --

Admiral Rogers: Sir.

Senator Peters: -- issues, as well.
I'd like to talk a little bit more about the future of warfare and the future of technology. There's been some questions related to machine learning and artificial intelligence, which is going to change everything, not just in the military space, but in the commercial side. I am on the Commerce Committee, and we recently had a hearing on artificial intelligence and how that's going to change business and commercial activities, in general. And I asked one of the leading executives at one of the leading technology companies in the country, What did he fear most about artificial intelligence? We had a hearing primarily of all the positive aspects of it, but I asked him, What did he fear? And I was actually surprised by his answer. He said his fear was the manipulation of elections and the manipulation of public opinion that can undermine democracy, which I thought was a very interesting response from a leading tech company.

And so, I wanted to ask you a bit about that in the Department of Defense, and, more broadly, our posture when it comes to investing in these technologies, and how are we working to increase innovation and work with those commercial companies to integrate it into defense systems? And I guess I'll ask you that question, as well. What do you fear -- if we don't get this right, what is our fear of an adversary acquiring machine learning and AI systems in
advance of our own capabilities?

Admiral Rogers: From a military's perspective, my concern is, you potentially lose speed and knowledge. That's a terrible combination as a warrior. Like, speed and knowledge are advantages for us, historically. And one of my concerns is, if we're not careful, AI potentially gives opponents speed and knowledge better than ours, if we're not careful. I'm not arguing that's going to happen, but I acknowledge we've got to look at it.

What was -- I apologize, Senator -- what was the --

Senator Peters: That's all right. That's -- and I guess I want to pick that up, because this technology is moving through the commercial side even --

Admiral Rogers: Right.

Senator Peters: -- faster than through the military side. So, it -- in the past, oftentimes military research would be a leading factor. That's not necessarily the case here at all. And I'm worried, in particular, about our adversaries that are able to come in and actually buy those technologies, particularly from startup companies.

Admiral Rogers: Right.

Senator Peters: I'm working right now in trying to fill some of the gaps on the CFIUS process, which is the Committee on Foreign Investment in the United States.

Admiral Rogers: Sir.
Senator Peters: You basically have foreign entities that buy companies, perfectly legal, get that information, and they use it not just for commercial applications, but also figure out ways to --

Admiral Rogers: Right.

Senator Peters: -- weaponize that type of technology, as well.

So, my question to you is, How can we better integrate the missions of CYBERCOM and the NSA as to it relates to this CFIUS review process? Are you concerned about it? What should we be doing to make sure that we are protecting this intellectual capital that has significant national defense potential?

Admiral Rogers: I'm not concerned about the review process, in terms of NSA role and Cyber Command. Again, it's one of the advantages of -- we are so physically colocated to each other.

My bigger concern goes to what you've already said. CFIUS, to me, is a reflection of an environment of the past, not today in the future. And it is very clear to me that some nation-states have spent a lot of time studying this CFIUS process, and have developed strategies to overcome it, "Hey, I don't have to worry about buying a corporation outright, it's -- so tell me what your oversea subsidiaries are, and tell me what your providers are, tell me who else
has access to this intellectual property, so to speak. I'll acquire that." And things like that, I'm going -- CFIUS is not set up to -- it wasn't what we built it to do. So, I applaud your efforts to -- we need a different construct. Not -- we don't want to get rid of CFIUS, but I need -- I think we need to think about it more broadly, about the national security challenges of foreign investment in areas with national security implications for us.

Senator Peters: Is there a role for CYBERCOM to be more actively involved in some of that process, providing information? I mean, you'll be aware of what's happening, things that you're concerned about, but how --

Admiral Rogers: Right.

Senator Peters: -- how do you see a potential role there, if any?

Admiral Rogers: I think it's much more an intelligence -- so, my role in -- on the NSA side, because we're tasked with generating knowledge and insight, is much greater. Cyber Command helps feeds -- feeds that effort, because one of the things we do is, we generate knowledge and insight on the Cyber Command side, based on what we're doing. We're putting out reporting, so that goes into the broader effort. But, it's not a primary mission for Cyber Command. It's much more a primary mission on the NSA side.

Senator Peters: Great. Thank you for your testimony.
Appreciate it.

Senator Inhofe: Senator Warren.

Senator Warren: Thank you, Mr. Chairman.

And, Admiral, thank you for your --

Admiral Rogers: Ma'am.

Senator Warren: -- 37 years of service. I --

Admiral Rogers: When you say that, I just feel --

[Laughter.]

Senator Warren: No, no, you should feel proud. Feel strong.

You know, you probably picked up on a theme today, that this committee feels a sense of urgency about the Russian threat to our elections. This is not a personal criticism of you.

Admiral Rogers: No, I understand.

Senator Warren: We're frustrated that this administration has not lived up to its responsibility to do something about the Russian cyber action.

Now, you told Senator Blumenthal and Senator McCaskill that not every cyberattack requires a cyber response. So, I'd just like to follow up on that just a little bit here.

The Pentagon's Cyber Security Strategy says -- and I'm going to quote it to you -- "In response to certain attacks and intrusions, the United States may undertake diplomatic actions, take law enforcement actions, and consider economic
sanctions." So, I want to focus for just a minute on that last piece, sanctions.

Congress overwhelmingly passed a law last year that, in part, required sanctions on individuals and companies that knowingly engage in malicious cyberactivities on behalf of the Russian government. Those sanctions include freezing access and restricting travel. The Trump administration has not imposed these required sanctions.

Admiral Rogers, I know that this is not your primary responsibility --

Admiral Rogers: Yes, ma'am.

Senator Warren: -- to impose the sanctions, but I want to ask a different question. What message does it send to Vladimir Putin that the United States has not fully implemented sanctions to counter known Russian cyberattacks?

Admiral Rogers: You know, more broadly, the -- not just the sanctions, but more broadly -- my concern is, I believe that President Putin has clearly come to the conclusion, "There's little price to play here" --

Senator Warren: Bingo.

Admiral Rogers: -- "and that, therefore, I can continue this activity."

Senator Warren: Yes.

Admiral Rogers: Everything, both as a director of NSA and what I see on the Cyber Command side, leads me to
believe that, if we don't change the dynamic here, this is
going to continue, and 2016 won't be viewed as something
isolated. This is something -- will be sustained over time.
So, I think the challenge for all of us is, So what are the
tools available to us? And, as the strategy says --
diplomatic, economic, some cyber things -- there are tools
available to us. And again, I think, in fairness, you can't
say nothing's been done. But, my point would be, it hasn't
been enough.

Senator Warren: It hasn't been enough.
Admiral Rogers: Clearly what we've done hasn't been
enough. And --

Senator Warren: That's right.
Admiral Rogers: -- you know, I'm mindful of my role as
an operational commander, but --

Senator Warren: Yeah. No, I appreciate that. It
hasn't been enough. And it doesn't do us any good to have
tools in the toolbox if we don't pick them up and use them.
You know, Russia will keep trying to interfere in our
elections. And, if the Trump administration doesn't fully
implement sanctions, then we're not using every tool we can
to effectively deter Russia from undermining democracy in
the future.

Let me ask you one other question, if I can, Admiral.
It's clear that the United States needs to step up its cyber
game. And I want to follow up on a question from Senator Tillis. We've previously discussed the question of how to build a skilled cyber force. And you said that improving DOD's network defenses and building a cybersecurity culture depends on our ability to attract the most talented people out there. This committee is now considering reforms to the Defense Officer Personnel Management Act, or --

Admiral Rogers: Right.

Senator Warren: -- DOPMA, another one of our great acronyms -- love to talk about DOPMA -- which governs how we recruit and retain our military officers. So, with that in mind, Admiral, if you could make just one change to DOPMA to help attract the right technical talent for the cyber jobs of tomorrow, what would that be?

Admiral Rogers: I'd want to make -- within a military --

Senator Warren: Yes

Admiral Rogers: -- construct -- and, to be honest, we use the phrase DOPMA, because "DOPE-MA" --

Senator Warren: Okay.

Admiral Rogers: -- sounds terrible.

Senator Warren: I always think --

Admiral Rogers: In a military standpoint, it would probably be -- and the services are working their way through this, but I think we want to make sure that we have
got a mechanism for a professional cyberforce across a career, that this can't be viewed as something we do -- "Hey, we give you training, you do it for a few years, you go do something else, you know, then we bring you back, then you're gone again." That's not going to get us where we need to be. And the services are all -- because they do man, train, and equip -- you know, they provide capability that I, as a joint -- and that includes people and other things -- but that I, as the joint commander, then harness to achieve specific mission outcomes as a joint commander. That would probably be the biggest thing.

Senator Warren: Okay. It's actually very helpful to know. I know that the 2017 defense bill gave the Pentagon a lot of flexibility in how to recruit, but I remain concerned that our recruiting system is so focused on recruiting for the military of today that we're not effectively targeting the best talent and best-suited talent to execute the missions we will face tomorrow. And so, how we think about that, I think, is really important.

Admiral Rogers: Ma'am.

Senator Warren: So, thank you again. Thank you for your service, and thank you for your help.

Admiral Rogers: Thank you, Senator.

Senator Warren: Thank you, Mr. Chairman.

Senator Inhofe: Thank you.

94

Alderson Court Reporting

www.aldersonreporting.com
It's the Chair's intention to go ahead and close the meeting after a few remarks from the Ranking Member. Is there objection to that?

[No response.]

Senator Inhofe: All right.

Senator Reed: Thank you very much, Mr. Chairman. I have just very specific points I want to clarify. First, there are ongoing Russian direct or inspired cyberoperations against our electoral system, as we speak?

Admiral Rogers: Yes, sir.

Senator Reed: Yes.

Admiral Rogers: Yes, sir. I'm speaking more as NSA than as Commander --

Senator Reed: Right.

Admiral Rogers: -- of Cyber Command, but yes, sir.

Senator Reed: Two, with the authority or the direction of the President of the United States, National Mission Teams can disrupt these attacks at the point of origin. Is that correct?

Admiral Rogers: We could be tasked to do that. Again, it depends on the specifics. I don't --

Senator Reed: But, it's legal?

Admiral Rogers: -- want to overpromise --

Senator Reed: It's legal, and it can be done.

Admiral Rogers: Sir.
Senator Reed: Have you been asked to make a recommendation to -- with respect to deploying these teams?

Admiral Rogers: No, but I've certainly provided my -- nobody's necessarily directly asked me -- I certainly have provided my opinion in ongoing discussions --

Senator Reed: What is your --

Admiral Rogers: -- about this.

Senator Reed: -- opinion?

Admiral Rogers: Again, my comment has been: Be mindful of just defaulting to the cyber piece, here. I'd like us to think about this a little bit more broadly, and I'd like us to think about, So how does this potential cyber piece that Cyber Command could play -- how does it fit into something broader?

Senator Reed: So, let's just conclude. You have not been formally asked for a recommendation.

Admiral Rogers: No, sir.

Senator Reed: You have expressed your opinion to the Secretary of Defense and to the White House about the possible uses of this, but not in any formal way.

Admiral Rogers: Yes, sir. I haven't put anything in writing, for example.

Senator Reed: And, I guess, final point. And this goes -- do you feel, as a professional officer, you have an obligation to make a formal recommendation to this? Have --
Admiral Rogers: I feel that the system provides me the opportunity to provide my recommendation, to provide my insights, to provide my opinions, that people listen to what I have to -- I acknowledge there's other opinions out there. I acknowledge there's other perspectives. But, I feel very comfortable in the fact that there's a -- been a dialogue on this topic, and that dialogue continues.

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

Senator Inhofe: Thank you.
And thank you, Admiral, for your straightforward answers and for the -- your patience on this, perhaps your last event here.

We are adjourned.

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