Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

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

Tuesday, April 5, 2016

Washington, D.C.

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

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

Tuesday, April 5, 2016

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

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

Committee Members Present: Senators McCain [presiding], Inhofe, Sessions, Ayotte, Fischer, Cotton, Rounds, Ernst, Tillis, Graham, Reed, Nelson, McCaskill, Manchin, Shaheen, Gillibrand, Blumenthal, Donnelly, Hirono, Kaine, King, and Heinrich.

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

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

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

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

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

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

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

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

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

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

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

Senator Reed.

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

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

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

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

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

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

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

interested in your thoughts on this very difficult issue.

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

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

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

Chairman McCain: Admiral Rogers, welcome back.

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

Admiral Rogers: Thank you, sir. Good to be back.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[The prepared statement of Admiral Rogers follows:]

Chairman McCain: Well, thank you, Admiral Rogers.

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

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

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

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

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

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

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

Admiral Rogers: Sir.

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

Admiral Rogers: Yes.

Chairman McCain: Does China have the same capability?

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

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

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

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

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

Admiral Rogers: Yes.

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

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

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

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

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

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

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

Admiral Rogers: In terms of --

Chairman McCain: Of action --

Admiral Rogers: -- cyber, overall?

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

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

Chairman McCain: Which --

Admiral Rogers: -- combat and weapon --

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

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

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

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

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

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

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

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

Chairman McCain: Senator Reed.

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

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

Admiral Rogers: Yes.

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

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

Senator Reed: Right.

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

priority to merit coordination across the entire Department?

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

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

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

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

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

Admiral Rogers: Yes.

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

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

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

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

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

[Laughter.]

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

Senator Reed: Right.

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

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

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

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

Senator Reed: Thank you.

Thank you, Mr. Chairman.

Chairman McCain: Senator Inhofe.

Senator Inhofe: Thank you, Mr. Chairman.

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

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

Senator Inhofe: Yeah.

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

Senator Inhofe: Yeah.

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

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

Senator Inhofe: Okay.

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

Senator Inhofe: Well --

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

Senator Inhofe: Sure.

Admiral Rogers: -- range; anywhere from --

Senator Inhofe: Sure.

Admiral Rogers: -- 20 to 60 --

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

Admiral Rogers: Yes, sir.

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

Admiral Rogers: Right.

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

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

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

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

Senator Inhofe: Yeah.

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

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

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

Admiral Rogers: Sir.

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

Admiral Rogers: No, sir.

Senator Inhofe: -- area. Okay, good.

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

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

Admiral Rogers: No, I'm not.

Senator Inhofe: Oh.

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

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

Admiral Rogers: Sir.

Senator Inhofe: Thank you, Mr. Chairman.

Chairman McCain: Senator Manchin.

Senator Manchin: Thank you, Mr. Chairman.

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

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

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

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

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

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

Admiral Rogers: Right.

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

Admiral Rogers: Yes, sir.

Senator Manchin: -- alarming concerns.

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

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

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

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

Admiral Rogers: Right.

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

Admiral Rogers: Right.

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

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

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

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

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

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

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

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

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

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

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

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

Senator Manchin: I'm just trying to --

Admiral Rogers: -- users out there.

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

Admiral Rogers: Yes, sir.

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

Admiral Rogers: Not like that.

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

Thank you for your service.

Admiral Rogers: Sir.

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

Admiral Rogers: Thanks, Senator.

Chairman McCain: Senator Sessions.

Senator Sessions: Thank you, Mr. Chairman.

And, Admiral Rogers --

Admiral Rogers: Sir.

Senator Sessions: -- thank you for your service. You're, I believe, the right person at a very challenging time, here in the middle of some decisions that have to be made by the United States sooner rather than later.

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

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

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

Admiral Rogers: Sir.

[The information referred to follows:]

[COMMITTEE INSERT]

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

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

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

Admiral Rogers: Right.

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

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

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

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

Senator Sessions: That's a good --

Admiral Rogers: -- describe the --

Senator Sessions: -- word.

Admiral Rogers: -- to describe that --

Senator Sessions: Supply-chain vulnerability, okay.

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

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

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

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

Admiral Rogers: Sir.

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

Admiral Rogers: Sir.

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

Admiral Rogers: Roger that.

Chairman McCain: Senator King.

Senator King: Thank you, Mr. Chairman.

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

Admiral Rogers: So, DOD has a responsibility to

defend critical infrastructure against events of significant cyber consequence.

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

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

Senator King: But, in terms of national defense,

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

Admiral Rogers: Sir.

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

Admiral Rogers: Criminal.

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

Admiral Rogers: Yes, sir.

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

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

sector? It's much bigger than just --

Senator King: Right.

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

Senator King: Well, I think --

Admiral Rogers: -- just the DOD.

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

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

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

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

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

Admiral Rogers: Yes, sir.

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

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

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

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

date.

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

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

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

Admiral Rogers: I do, sir.

Senator King: Yes, sir. Thank you.

Thank you, Mr. Chairman.

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

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

Chairman McCain: Thank you.

Senator Fischer.

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

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

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

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

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

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

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

Admiral Rogers: Oh, yes, ma'am.

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

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

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

Admiral Rogers: Yes, ma'am.

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

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

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

Senator Fischer: Well, it's --

Admiral Rogers: -- literally --

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

Admiral Rogers: Right, decades of investment we're

trying to overcome.

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

Admiral Rogers: Yes.

Senator Fischer: Thank you very much.

Admiral Rogers: Yes, ma'am.

Chairman McCain: Senator Blumenthal.

Senator Blumenthal: Thanks, Mr. Chairman.

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

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

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

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

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

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

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

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

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

Admiral Rogers: Right. Right.

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

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

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

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

Admiral Rogers: Right. Power is an example.

Senator Blumenthal: Yeah.

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

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

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

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

Senator Blumenthal: Thank you very much.

Admiral Rogers: Sir.

Senator Blumenthal: Thank you, Mr. Chairman.

Chairman McCain: Senator Rounds.

Senator Rounds: Thank you, Mr. Chairman.

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

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

Admiral Rogers: Right.

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

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

Senator Rounds: The --

Admiral Rogers: I just haven't --

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

Admiral Rogers: Yes.

Senator Rounds: Fair to --

Admiral Rogers: Yes.

Senator Rounds: -- look at it?

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

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

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

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

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

Admiral Rogers: Right.

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

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

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

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

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

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

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

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

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

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

Senator Rounds: But, not one that --

Admiral Rogers: -- political decision.

Senator Rounds: -- could be done in milliseconds.

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

Senator Rounds: Thank you. Thank you, sir.

Thank you, Mr. Chairman.

Chairman McCain: Senator McCaskill.

Senator McCaskill: Thank you, Mr. Chairman.

Thank you, Admiral, for being here.

Admiral Rogers: Senator.

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

dollars wasted?

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

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

Admiral Rogers: Yes, ma'am.

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

Admiral Rogers: Oh, yes, ma'am.

Senator McCaskill: -- the underlying --

Admiral Rogers: You have to buy the right --

Senator McCaskill: -- the capabilities.

Admiral Rogers: -- capabilities.

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

Admiral Rogers: Yes, ma'am.

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

[The information referred to follows:]

[COMMITTEE INSERT]

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

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

Senator McCaskill: Obviously.

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

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

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

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

Admiral Rogers: Yes, ma'am.

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

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

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

Admiral Rogers: Right.

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

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

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

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

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

Senator McCaskill: Thank you, Admiral.

Admiral Rogers: Yes, ma'am.

Chairman McCain: Senator Graham.

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

Admiral Rogers: Yes, sir.

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

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

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

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

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

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

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

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

Senator Graham: Do you think the Russian government's

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

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

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

Admiral Rogers: Yes.

Senator Graham: Are they less threatening?

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

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

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

Senator Graham: They're improving their capability?

Admiral Rogers: Yes, sir.

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

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

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

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

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

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

Admiral Rogers: -- domain --

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

Admiral Rogers: -- for our Nation.

Senator Graham: -- so let's march down that path. And I associate myself with Senator King about what we need to do as a Nation.

Admiral Rogers: Sir.

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

Admiral Rogers: Yes, sir.

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

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

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

Admiral Rogers: Not nearly the same.

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

Admiral Rogers: Oh, significant.

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

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

Senator Graham: Are the Iranians trying to close it?

Admiral Rogers: Oh, they are.

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

Admiral Rogers: Sir.

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

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

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

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

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

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

Senator Graham: What's the biggest impediment to us getting there? Is it the Congress? Is it the --

Admiral Rogers: No.

Senator Graham: -- DOD?

Admiral Rogers: It's as much, in some ways, as -- and again, this is just Mike Rogers' opinion -- it's as much, in some ways, from my perspective, as, "Well, this is just an intellectual exercise. It -- this is something we can afford to" --

Senator Graham: The Department --

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

Senator Graham: -- of Homeland Security is responsible, basically, for protecting us in the financial/service/power arena, our civilian targets.

Admiral Rogers: Sir.

Senator Graham: You're responsible for protecting the military infrastructure.

Admiral Rogers: And we provide support to that commercial --

Senator Graham: That's right.

Admiral Rogers: -- infrastructure, if requested.

Senator Graham: But, you're also responsible for going on offense. The --

Admiral Rogers: Yes, sir.

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

Admiral Rogers: Yes, sir.

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

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

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

Admiral Rogers: Yes, sir.

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

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

Senator Graham: How do they respond?

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

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

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

Senator Graham: Thank you.

Admiral Rogers: Sir.

Chairman McCain: Senator Hirono.

Senator Hirono: Thank you, Mr. Chairman.

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

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

Admiral Rogers: Well --

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

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

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

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

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

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

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

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

to partner together a lot.

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

Admiral Rogers: Right.

Senator Hirono: -- effort.

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

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

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

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

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

Admiral Rogers: Right.

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

Admiral Rogers: Yes, ma'am.

Senator Hirono: Thank you, Mr. Chairman.

Chairman McCain: Senator Tillis.

Senator Tillis: Thank you, Mr. Chairman.

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

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

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

Admiral Rogers: Right.

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

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

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

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

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

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

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

Admiral Rogers: Sure.

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

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

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

Admiral Rogers: Right.

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

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

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

Admiral Rogers: Sure.

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

Admiral Rogers: Oh, yes, sir.

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

Thank you very much.

Chairman McCain: Senator Reed.

Senator Reed: Thank you, Mr. Chairman.

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

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

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

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

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

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

Chairman McCain: But, explain the first one.

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

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

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

Chairman McCain: Senator Shaheen.

Senator Shaheen: Thank you, Mr. Chairman.

And thank you --

Admiral Rogers: Senator.

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

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

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

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

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

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

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

Admiral Rogers: Yes, ma'am.

Senator Shaheen: -- classified setting.

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

Admiral Rogers: Right.

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

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

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

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

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

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

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

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

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

Admiral Rogers: The Defense League.

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

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

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

Senator Shaheen: Right.

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

Senator Shaheen: Right.

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

Senator Shaheen: Right.

Admiral Rogers: -- private-sector capabilities.

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

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

Senator Shaheen: Right.

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

Senator Shaheen: Thank you.

Thank you, Mr. Chairman.

Chairman McCain: Senator Ayotte.

Senator Ayotte: Thank you, Chairman.

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

Admiral Rogers: Senator.

Senator Ayotte: -- to the country.

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

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

[Laughter.]

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

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

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

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

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

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

Senator Ayotte: Power system --

Admiral Rogers: Power systems.

Senator Ayotte: -- financial system.

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

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

Admiral Rogers: Yes, ma'am.

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

Admiral Rogers: Right.

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

Admiral Rogers: Oh, the --

Senator Ayotte: -- the USA Freedom Act --

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

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

Admiral Rogers: Right.

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

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

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

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

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

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

Admiral Rogers: In some ways, it takes longer.

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

Admiral Rogers: Yes, ma'am.

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

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

Admiral Rogers: Yeah, the Iran --

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

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

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

Senator Ayotte: -- this agreement?

Admiral Rogers: -- I cannot speak for the U.S. Government as a whole. I can tell you U.S. Cyber Command has not participated in any such effort.

Senator Ayotte: Okay. Thank you.

Admiral Rogers: Yes, ma'am.

Chairman McCain: Senator Kaine.

Senator Kaine: Thank you, Mr. Chair.

Thank you, Admiral Rogers.

Admiral Rogers: Senator.

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

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

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

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

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

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

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

Admiral Rogers: Right.

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

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

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

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

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

Admiral Rogers: Right.

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

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

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

Senator Kaine: Siloed.

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

Senator Kaine: Great. Thank you.

Thanks, Mr. Chair.

Chairman McCain: Senator Cotton.

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

Admiral Rogers: Sir.

Senator Cotton: -- the committee.

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

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

Admiral Rogers: Yes, sir.

Senator Cotton: Yeah. Are --

Admiral Rogers: Yes, sir.

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

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

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

Admiral Rogers: Yes, sir.

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

Admiral Rogers: Yes, sir.

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

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

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

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

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

Senator Cotton: Okay.

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

Chairman McCain: He's ahead of Senator Graham.

[Laughter.]

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

Admiral Rogers: Right.

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

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

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

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

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

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

Admiral Rogers: Act.

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

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

Senator Cotton: Okay.

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

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

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

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

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

Senator Cotton: Thank you.

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

Admiral Rogers: Yes.

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

acts of terrorism.

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

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

Admiral Rogers: Yes, sir.

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

Admiral Rogers: So, I --

Chairman McCain: Besides take out ISIS.

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

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

Admiral Rogers: Yes, sir.

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

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

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

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

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

Admiral Rogers: Yes.

Chairman McCain: Senator King.

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

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

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

Is that correct, Admiral?

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

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

outstanding and highly selected individuals.

Admiral Rogers: Yes.

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

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

Hearing is adjourned.

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