May 9, 2017

United States Cyber Command

Committee on Armed Services, United States Senate, One Hundred Fifteenth Congress, First Session

---

Hearing Contents:

Member Statements

Witnesses

Admiral Michael S. Rogers, United States Navy
Commander, United States Cyber Command
Director, National Security Agency
Chief, Central Security Services
View Testimony

Available Webcast(s)*:

Watch Full Hearing

Compiled From*:

https://www.armed-services.senate.gov/hearings/17-05-09-united-states-cyber-command

** Please Note: External links included in this compilation were functional at the time of its creation but are not maintained thereafter.*

Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON UNITED STATES

CYBER COMMAND

Tuesday, May 9, 2017

Washington, D.C.

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

HEARING TO RECEIVE TESTIMONY ON

UNITED STATES CYBER COMMAND

Tuesday, May 9, 2017

U.S. Senate

Committee on Armed Services

Washington, D.C.

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

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

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

Chairman McCain: Good morning.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Senator Reed?

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

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

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

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

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

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

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

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

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

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

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

Thank you, Mr. Chairman.

Chairman McCain: Welcome back, Admiral.

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[The prepared statement of Admiral Rogers follows:]

Chairman McCain: Thank you, Admiral.

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

Admiral Rogers: No, I do not.

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

Admiral Rogers: No, I have not.

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

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

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

Admiral Rogers: Yes, sir.

Chairman McCain: Do we have that now?

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

Chairman McCain: And the check is in the mail?

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

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

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

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

Chairman McCain: Do we need a cyber corps?

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

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

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

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

Chairman McCain: Was that message received by the

United States Air Force?

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

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

Admiral Rogers: For?

Chairman McCain: For cyber attacks on the United States.

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

Chairman McCain: Including space?

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

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

Chairman McCain: Like changing voting rolls.

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

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

Chairman McCain: And the best.

Admiral Rogers: The best is --

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

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

Chairman McCain: Thank you, Admiral.

Senator Reed?

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

Again, thank you, Admiral.

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

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

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

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

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

Senator Reed: That is fine.

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

step back and reassess that.

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

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

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

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

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

Admiral Rogers: Broadly.

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

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

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

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

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

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

Admiral Rogers: Yes, sir.

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

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

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

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

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

Admiral Rogers: Yes.

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

Admiral Rogers: I apologize, Senator.

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

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

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

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

Chairman McCain: Senator Inhofe?

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

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

Senator Inhofe: It has to come from somewhere.

Admiral Rogers: Yes, sir.

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

might be right on this.

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

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

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

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

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

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

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

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

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

Senator Inhofe: I kind of got that impression too.

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

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

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

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

Admiral Rogers: We are trying.

Senator Inhofe: Thank you very much.

Chairman McCain: Senator Nelson?

Senator Nelson: Thank you, Mr. Chairman.

And thank you, Admiral, for your public service.

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

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

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

The chairman mentioned and asked you is this what we

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

Admiral Rogers: Yes, sir.

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

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

Senator Nelson: Both.

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

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

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

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

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

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

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

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

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

just used -- "deterrence" -

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

Senator Nelson: That would be very helpful.

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

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

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

Admiral Rogers: Yes, sir.

Senator Nelson: And that is critical infrastructure.

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

Senator Nelson: Thank you, Mr. Chairman.

Chairman McCain: Senator Wicker?

Senator Wicker: Thank you.

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

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

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

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

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

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

Senator Wicker: Right.

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

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

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

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

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

by most nations around the world.

Senator Wicker: Well, keep us posted on that.

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

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

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

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

Senator Wicker: How are we going to do that?

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

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

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

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

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

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

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

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

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

Admiral Rogers: Yes, sir.

Chairman McCain: Senator Gillibrand?

Senator Gillibrand: Thank you, Mr. Chairman.

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

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

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

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

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

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

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

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

Senator Gillibrand: Correct.

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

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

it is not adequate.

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

Admiral Rogers: Yes, ma'am.

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

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

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

Senator Gillibrand: Agreed.

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

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

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

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

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

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

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

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

Senator Gillibrand: Thank you, Admiral.

Admiral Rogers: Yes, ma'am.

Chairman McCain: Senator Fischer?

Senator Fischer: Thank you, Mr. Chairman.

Thank you, Admiral, for being here today.

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

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

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

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

PPD-20, for example.

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

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

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

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

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

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

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

Senator Fischer: Is the Department reviewing it?

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

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

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

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

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

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

Senator Fischer: Okay.

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

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

The argument I am trying to make is building on the

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

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

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

Senator Fischer: Can we do that now?

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

Senator Fischer: Thank you.

Thank you, Mr. Chairman.

Chairman McCain: Senator King?

Senator King: Thank you, Mr. Chairman.

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

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

[The information follows:]

[COMMITTEE INSERT]

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

Admiral Rogers: Yes, sir.

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

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

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

issue than me.

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

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

Admiral Rogers: I agree.

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

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

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

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

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

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

Admiral Rogers: Yes, sir.

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

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

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

[Laughter.]

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

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

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

Admiral Rogers: Right.

Senator King: Thank you.

Thank you, Mr. Chairman.

Chairman McCain: Senator Rounds?

Senator Rounds: Thank you, Mr. Chairman.

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

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

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

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

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

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

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

identified investments in manpower as well.

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

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

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

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

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

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

Admiral Rogers: No, no. I understand.

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

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

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

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

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

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

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

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

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

Senator Rounds: Thank you, sir.

Thank you, Mr. Chairman.

Chairman McCain: Senator Heinrich?

Senator Heinrich: Thank you, Chairman.

Welcome back, Admiral Rogers.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Admiral Rogers: Yes, sir.

Senator Heinrich: Thank you.

Chairman McCain: Senator Ernst?

Senator Ernst: Thank you.

Admiral Rogers, it is good to see you again.

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

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

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

capabilities? What else can we do?

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

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

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

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

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

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

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

Admiral Rogers: Can I make one other point? I

apologize. I did not mean to interrupt.

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

Senator Ernst: Yes.

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

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

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

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

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

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

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

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

Thank you, Mr. Chair.

Chairman McCain: Senator Hirono?

Senator Hirono: Thank you, Mr. Chairman.

The Office of the Director of National Intelligence

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Senator Hirono: And in your meetings with the other

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

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

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

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

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

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

Chairman McCain: Senator Tillis?

Senator Tillis: Thank you, Mr. Chair.

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

Admiral Rogers: 3 years, sir.

Senator Tillis: 3.

Admiral Rogers: Yes, sir.

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

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

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

Admiral Rogers: Right.

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

Admiral Rogers: Narrowing. The gap is narrowing.

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

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

last 3 years since you have been in the position?

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

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

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

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

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

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

Senator Tillis: Is that within your current

authorities?

Admiral Rogers: I am sorry, sir?

Senator Tillis: Is that within current authorities?

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

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

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

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

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

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

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

Senator Tillis: Thank you.

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

Senator Warren: Thank you.

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

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

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

Admiral Rogers: Tougher.

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

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

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

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

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

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

Senator Warren: I understand.

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

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

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

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

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

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

important here.

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

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

Senator Warren: Good.

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

Admiral Rogers: Yes, ma'am.

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

Admiral Rogers: Thanks.

Chairman McCain [presiding]: Senator Perdue?

Senator Perdue: Thank you, Mr. Chair.

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

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

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

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

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

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

Senator Perdue: I understand.

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

Admiral Rogers: So we will transition to that model in

2018. The initial outfit, if you will, of the Cyber Mission Force, using much of NSA's infrastructure -- we signed up, speaking now as the Director of NSA, to use much of NSA's structure, our schoolhouses, our National Cryptologic School, for ex4ample, to do much, not all, but to do much of the training associated with the initial build-out of the mission force. That build-out, full operating capability is due to be completed, and we are on track for 30 September 2018. The agreement then was at that point responsibility for training and development, long-term sustainment of the force would transition to a service structure. We are on track to do that right now.

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

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

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

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

Senator Perdue: I understand. I get it.

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

Admiral Rogers: Right. Yes, sir.

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

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

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

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

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

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

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

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

has penetrated a system.

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

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

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

Senator Perdue: Thank you, Admiral.

Chairman McCain: Senator Peters?

Senator Peters: Thank you, Mr. Chairman.

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

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

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

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

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

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

Senator Peters: Do you feel that CFIUS is adequately

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

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

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

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

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

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

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

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

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

We also do regular tabletop exercises where we talk at

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

Senator Peters: Thank you, Admiral.

Chairman McCain: Senator Cotton?

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

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

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

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

Could you explain the discrepancy for us?

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

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

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

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

Admiral Rogers: Correct.

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

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

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

Admiral Rogers: Yes, sir.

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

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

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

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

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

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

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

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

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

be happy about.

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

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

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

Senator Cotton: Thank you very much.

Chairman McCain: Senator Kaine?

Senator Kaine: Thank you, Mr. Chair.

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

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

Senator Kaine: High confidence in that.

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

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

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

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

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

Admiral Rogers: Yes, sir.

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

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

Admiral Rogers: Yes, sir.

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

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

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

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

Admiral Rogers: A foreign counterpart?

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

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

Admiral Rogers: We need to be concerned.

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

[The information follows:]

[COMMITTEE INSERT]

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

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

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

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

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

Senator Kaine: All right.

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

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

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

Senator Kaine: Thank you, Admiral.

Thank you, Mr. Chairman.

Chairman McCain: Senator Graham?

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

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

Admiral Rogers: Yes.

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

Admiral Rogers: Yes.

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

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

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

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

Admiral Rogers: Yes.

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

Admiral Rogers: Yes.

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

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

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

Senator Graham: Can we build that out a bit?

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

Yes, sir.

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

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

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

Admiral Rogers: Yes, sir.

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

Admiral Rogers: Yes, sir.

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

Admiral Rogers: I think we have publicly acknowledged --

Senator Graham: Around 2,000.

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

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

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

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

Senator Graham: I got you.

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

Admiral Rogers: In terms of authorizing the unmasking?

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

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

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

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

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

Admiral Rogers: Yes.

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

citizen.

Admiral Rogers: Yes, sir.

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

Admiral Rogers: Yes, sir.

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

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

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

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

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

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

Senator Graham: Assuming he did not have a FISA

warrant allowing us to collect on him, it would be a case of incidental collection following the Russian ambassador. Does that sense?

Admiral Rogers: Yes, sir.

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

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

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

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

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

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

Senator Graham: Of incidental collection?

Admiral Rogers: Incidental with U.S. persons.

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

Admiral Rogers: Yes, sir.

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

"Washington Post."

Admiral Rogers: Somehow it got to the media.

Senator Graham: That is a crime.

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

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

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

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

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

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

Senator Graham: Do you know is Susan Rice ever asked

for an American citizen to be unmasked?

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

Senator Graham: Thank you.

Chairman McCain: Senator Blumenthal?

Senator Blumenthal: Thanks, Mr. Chairman.

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

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

Admiral Rogers: Yes, sir.

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

Admiral Rogers: Certainly nothing that is changing their behavior.

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

Admiral Rogers: Yes, sir.

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

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

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

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

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

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

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

just not my lane in the road.

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

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

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

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

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

Admiral Rogers: Yes, sir.

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

Admiral Rogers: Right.

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

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

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

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

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

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

Senator Blumenthal: Thank you.

Thanks, Mr. Chairman.

Chairman McCain: Senator McCaskill?

Senator McCaskill: Thank you, Mr. Chairman.

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

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

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

In the United Kingdom, the NCSC has real-time

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

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

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

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

[The information follows:]

[COMMITTEE INSERT:}

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

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

Senator McCaskill: Sure.

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

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

Admiral Rogers: Right, now.

Senator McCaskill: -- responsibility.

Admiral Rogers: Yes, ma'am. Now.

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

I guess it seems to me that when someone is impacting

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

Admiral Rogers: Right.

Senator McCaskill: Forget about Russia for a minute. Are you familiar with the UK model?

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

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

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

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

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

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

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

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

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

Senator McCaskill: I get it.

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

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

Admiral Rogers: Yes, Senator.

Senator McCaskill: Thank you, Admiral.

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

Senator Shaheen: Thank you, Mr. Chairman.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Admiral Rogers: That is not what I said.

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

Admiral Rogers: Yes, ma'am.

Senator Reed: Thank you.

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

communicate to your colleagues our appreciation for their service also?

On behalf of Chairman McCain, the hearing is adjourned.

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

Stenographic Transcript
Before the

COMMITTEE ON
ARMED SERVICES

UNITED STATES SENATE

HEARING TO RECEIVE TESTIMONY ON UNITED STATES

CYBER COMMAND

Tuesday, May 9, 2017

Washington, D.C.

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

HEARING TO RECEIVE TESTIMONY ON

UNITED STATES CYBER COMMAND

Tuesday, May 9, 2017

U.S. Senate

Committee on Armed Services

Washington, D.C.

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

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

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

Chairman McCain: Good morning.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Senator Reed?

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

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

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

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

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

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

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

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

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

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

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

Thank you, Mr. Chairman.

Chairman McCain: Welcome back, Admiral.

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[The prepared statement of Admiral Rogers follows:]

Chairman McCain: Thank you, Admiral.

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

Admiral Rogers: No, I do not.

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

Admiral Rogers: No, I have not.

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

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

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

Admiral Rogers: Yes, sir.

Chairman McCain: Do we have that now?

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

Chairman McCain: And the check is in the mail?

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

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

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

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

Chairman McCain: Do we need a cyber corps?

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

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

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

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

Chairman McCain: Was that message received by the

United States Air Force?

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

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

Admiral Rogers: For?

Chairman McCain: For cyber attacks on the United States.

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

Chairman McCain: Including space?

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

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

Chairman McCain: Like changing voting rolls.

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

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

Chairman McCain: And the best.

Admiral Rogers: The best is --

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

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

Chairman McCain: Thank you, Admiral.

Senator Reed?

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

Again, thank you, Admiral.

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

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

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

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

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

Senator Reed: That is fine.

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

step back and reassess that.

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

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

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

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

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

Admiral Rogers: Broadly.

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

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

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

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

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

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

Admiral Rogers: Yes, sir.

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

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

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

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

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

Admiral Rogers: Yes.

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

Admiral Rogers: I apologize, Senator.

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

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

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

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

Chairman McCain: Senator Inhofe?

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

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

Senator Inhofe: It has to come from somewhere.

Admiral Rogers: Yes, sir.

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

might be right on this.

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

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

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

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

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

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

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

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

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

Senator Inhofe: I kind of got that impression too.

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

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

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

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

Admiral Rogers: We are trying.

Senator Inhofe: Thank you very much.

Chairman McCain: Senator Nelson?

Senator Nelson: Thank you, Mr. Chairman.

And thank you, Admiral, for your public service.

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

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

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

The chairman mentioned and asked you is this what we

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

Admiral Rogers: Yes, sir.

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

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

Senator Nelson: Both.

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

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

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

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

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

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

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

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

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

just used -- "deterrence" -

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

Senator Nelson: That would be very helpful.

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

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

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

Admiral Rogers: Yes, sir.

Senator Nelson: And that is critical infrastructure.

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

Senator Nelson: Thank you, Mr. Chairman.

Chairman McCain: Senator Wicker?

Senator Wicker: Thank you.

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

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

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

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

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

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

Senator Wicker: Right.

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

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

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

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

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

by most nations around the world.

Senator Wicker: Well, keep us posted on that.

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

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

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

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

Senator Wicker: How are we going to do that?

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

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

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

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

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

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

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

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

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

Admiral Rogers: Yes, sir.

Chairman McCain: Senator Gillibrand?

Senator Gillibrand: Thank you, Mr. Chairman.

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

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

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

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

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

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

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

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

Senator Gillibrand: Correct.

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

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

it is not adequate.

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

Admiral Rogers: Yes, ma'am.

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

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

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

Senator Gillibrand: Agreed.

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

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

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

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

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

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

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

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

Senator Gillibrand: Thank you, Admiral.

Admiral Rogers: Yes, ma'am.

Chairman McCain: Senator Fischer?

Senator Fischer: Thank you, Mr. Chairman.

Thank you, Admiral, for being here today.

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

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

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

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

PPD-20, for example.

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

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

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

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

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

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

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

Senator Fischer: Is the Department reviewing it?

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

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

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

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

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

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

Senator Fischer: Okay.

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

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

The argument I am trying to make is building on the

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

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

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

Senator Fischer: Can we do that now?

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

Senator Fischer: Thank you.

Thank you, Mr. Chairman.

Chairman McCain: Senator King?

Senator King: Thank you, Mr. Chairman.

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

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

[The information follows:]

[COMMITTEE INSERT]

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

Admiral Rogers: Yes, sir.

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

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

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

issue than me.

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

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

Admiral Rogers: I agree.

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

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

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

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

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

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

Admiral Rogers: Yes, sir.

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

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

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

[Laughter.]

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

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

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

Admiral Rogers: Right.

Senator King: Thank you.

Thank you, Mr. Chairman.

Chairman McCain: Senator Rounds?

Senator Rounds: Thank you, Mr. Chairman.

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

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

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

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

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

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

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

identified investments in manpower as well.

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

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

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

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

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

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

Admiral Rogers: No, no. I understand.

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

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

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

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

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

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

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

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

mission set, so to speak, but our success helps to underpin the ability of the rest of the Department. I am not saying it is the only determinant, but it is a foundational element of the Department's broader ability to execute its mission sets across the breadth of DOD missions.

Senator Rounds: Thank you, sir.

Thank you, Mr. Chairman.

Chairman McCain: Senator Heinrich?

Senator Heinrich: Thank you, Chairman.

Welcome back, Admiral Rogers.

It has become really evident to me as a member of both the Intel Committee and this committee -- it has become crystal clear that Russia has really mastered this domain of digital disinformation and that they have effectively set up a situation where they are coordinating paid trolls, fake automated social media accounts, bots, as they call them, and state-backed news outlets to really amplify stories very effectively that serve their interest. And that is true of what we would call fake news. It is also true of any real news that simply serves their interests or undermines U.S. policy.

So these capabilities are proving to be just as politically disruptive both in our elections and day-to-day business, as well as what we have seen in Europe, as to the Russian hacking that we have seen.

So does Cyber Command have a role to play in meeting this new what I would describe as a threat, not just a reality? Or do you see it as wholly outside your lane?

Admiral Rogers: I would not say it is wholly outside. There is a broader issue to me, and information is one aspect of it. If you look at, for example, the way the spectrum and the network world are converging, if you look at the way the information dynamic is playing out, one of the questions that we are trying to come to grips with broadly within the Department, although I will be the first to admit I am so focused right now on trying to execute the missions I have been assigned -- part of my input to this process has been let me get the structures set before we start throwing more stuff on the life raft.

But I am trying to conceptualize in my own mind, so how are we going to bring together electronic warfare, cyber, and the information dynamic because it is all blurring in this digital world that we are living in. And how do we do this in an integrated way? And right now, we are not there yet. We are still trying to figure out what is the right was forward.

Senator Heinrich: Do you have people assigned to look at, for example, just the issue of when you have thousands and thousands of bots out there and they serve as a forcing mechanism, they look like social media accounts in Wisconsin

or Michigan or somewhere else in the United States, but they are really just automated accounts that take a story that has interested 10 people and makes it look like it is of interest to 10,000. Suddenly it is on my social media feed or my news feed on my iPhone.

Have we looked at capabilities for simply making it clear, even to the companies whose platforms those are on, that those accounts are not genuine accounts? Because it seems to me if you take that amplification piece out, even if it is on a constant rolling basis, you would have a dramatically diminished impact from this.

Admiral Rogers: Yes, although there are couple points, if I could.

First, remember much of the scenario you just went through is about domestic and both as NSA and Cyber Command, we are focused largely -- NSA -- we are focused externally. Cyber Command we are largely focused externally. So I will monitor bots infrastructure external to the United States. When it comes to --

Senator Heinrich: Well, bot farms typically are overseas. However, they are appearing to be domestic accounts but they are not attached to actual people in the United States.

Admiral Rogers: But one of the phenomena we are starting to see is you are certain to see a migration of

capability from the external infrastructure that we have been aware of and observing for some period of time. The way this is going to go next in my opinion, you are going to start to see this in domestic manipulation. And that is a part that for us right now, no, I am not really directly involved in.

We do, as part of the broader government effort participate in generating insight that we share with major social media providers to say, hey, this is activity that we are seeing that we believe to be false or that we believe to be criminal or we believe to be supporting of particular groups that are a threat to the Nation.

Senator Heinrich: So you are actually able in relatively real time to share information with big social media providers.

Admiral Rogers: In some cases, and I would not argue that it is necessarily immediate real time because one of the things that I try to do is kind of get a critical center-- get enough that I can try to show them a comprehensive effort here as opposed to coming to them with, hey, here is the count today, here is 10 the next hour because we are in the early stage of this. I am trying to engender a broader dialogue about, look, there is systematic here that both of us have got to be looking at. We got to stop looking at this one individual --

Senator Heinrich: Exactly. And I think it speaks to the relationship you were talking about. Whether you are talking about the financial services sector, the utility sector, or in this case, social media and media, we need to have those relationships in place to be much more responsive than we currently are.

Admiral Rogers: Yes, sir.

Senator Heinrich: Thank you.

Chairman McCain: Senator Ernst?

Senator Ernst: Thank you.

Admiral Rogers, it is good to see you again.

During Senator Fischer's line of questioning, you had answered that you do not want to show up in the middle of a conflict, you do not want to have to learn about the enemy on the move. And I agree. And I would also say that conversely we also want to know about our friendlies, and we do not want to learn about them on the move either.

So going back to the National Guard, we have corresponded back and forth a number of times. And we want to make sure that you know about those friendlies and the capabilities that they bring into your organization, should they ever be needed. So I did drop a bill earlier this year to ensure that DOD will start tracking these capabilities.

But from your perspective, what more can we be doing to help CYBERCOM connect with our National Guard and their

capabilities? What else can we do?

Admiral Rogers: So I feel pretty good about knowledge and awareness. I never thought as a commander -- but I can walk you through what Kansas is doing, Pennsylvania is doing, Delaware, Virginia, Washington, California. Again, it is kind of interesting to me. I think to myself, wow, Rogers, you are in a very different world here.

The biggest challenge that I am still trying to work -- and it is one I have outlined about six different priorities for Cyber Command for calendar 2017. I said, hey, these are six things we are going to focus on. One of the six is about creating a model for Reserve and Guard integration. So I am trying to partner with Northern Command, as well as the National Guard Bureau, General Lengyel and his team, about, okay, so we are seeing the investments that the Guard and the Reserve is making, which I am very supportive of and appreciative of. Now, how do we create the mechanisms so we can actually apply that in real time?

We are doing some things now, for example, where Air Force is activating -- and in fact, I have reviewed the activation sequence in the Guard out to fiscal year 2020 for the Guard units we are going to bring on in active status to meet the requirements that the Air Force has for the Cyber Mission Force that I command, I lead.

But what I am trying to get to is if we have a major

cyber event, I feel very comfortable about we understand who is going to do what. What I am curious about is what happens if it is not something catastrophic, if it is not something that necessarily trips a threshold where the DOD active force is viewed as the primary responsibility. But how do we use those Guard and Reserve capabilities in instances where the active side is not necessarily going to be the lead? How do we make sure the capabilities are there? How do we apply them? What is the command and control structure that is in place?

We do that now in terms of defense support to civil authorities. That is very mature in terms of how we respond to natural disasters. We have got a great process there. Support to FEMA, the Northern Command's role. I am trying to argue we got to spend a little more time on the cyber piece of this.

Senator Ernst: Absolutely. I would agree wholeheartedly. Maybe it runs parallel to our civil support teams where they provide backup in case of any sort of incident, the Super Bowl, and things like that. We always have them on standby. And as we look at major events and progression, whether it is elections or other significant events, throughout the year, we have those Guard capabilities.

Admiral Rogers: Can I make one other point? I

apologize. I did not mean to interrupt.

One of the other challenges in the Guard construct, the Guard's construct is a geographic construct based on the State.

Senator Ernst: Yes.

Admiral Rogers: And so one of the challenges, again, I am trying to work my mind through -- and I had this discussion with the Council of Governors and the TAGs. In many instances, the infrastructure that a State is going to be counting on from a cyber perspective in the cyber arena does not necessarily physically reside in the State. So how do we take advantage of the Guard structure more broadly and not just -- I am not saying that the State piece is not important, but I am trying to figure how do we overlay a largely geographic and State-defined construct on something that is not always defined by immediate geography, if that makes sense.

Senator Ernst: It does make sense. It absolutely does make sense.

And I know a number of my colleagues, moving on to a different topic, have talked about personnel and how do we keep personnel there. So there have been a lot of suggestions about bringing civilians in to fill in the gaps.

But during Secretary Mattis' confirmation, he also stated that the warrior ethos is not a luxury. It is

essential when you have a military. And as we look at things like lateral accessions and flexible career paths, how do we make sure that warrior ethos is not being diluted?

Admiral Rogers: I am the first to admit. It is one reason why I have argued be leery of creating a cyber force that is predominantly civilian. No disrespect to my civilian teammates. But we want that warrior ethos and culture. Secondly, in the law of armed conflict, there were things legally that a uniformed military member of a nation state can do that a civilian cannot within a legal framework.

So civilians play an important role here. Do not get me wrong. And that is one of the reasons why I believe that the right construct for us is to bring the total spectrum, active, Guard, Reserve, contractor, civilian, private sector. It is our ability to bring it all together, not one single slice. So I would be leery about swinging the pendulum too far in one direction away from the military piece of that.

Senator Ernst: Thank you for laying that out. I appreciate your time, Admiral Rogers.

Thank you, Mr. Chair.

Chairman McCain: Senator Hirono?

Senator Hirono: Thank you, Mr. Chairman.

The Office of the Director of National Intelligence

released an intelligence community assessment on Russian activities and intentions in recent U.S. elections. And General Clapper testified regarding this report yesterday in the Judiciary subcommittee.

So we all know that Russia interfered with our elections. So do you view President Putin's actions in this regard as a cyber attack?

Admiral Rogers: Again, ma'am, that is a legal and a policy discussion. My point is it should be viewed as unacceptable. That is the bottom line to me. This is not a behavior you want to encourage. This is not a behavior we want to accept, nor is this a behavior I think we want to see repeated.

Senator Hirono: I think we all share that. How to get there is the challenge.

What is your opinion of the role of the military and intelligence agencies in preventing these types of events in the future?

Admiral Rogers: So, first, from an intelligence perspective, our job, speaking as the Director of NSA, is to generate insights and knowledge that help inform potential response and the ability also, if we can get ahead of the problem, to identify it in advance, intent, a nation where actors intend to do something, that then alarms policymakers and military commanders with the ability to engage in

operations or choices that clearly communicate to that other party, hey, we know what you are thinking about doing. You do not want to go down this road.

On the Cyber Command side, again, if we define election infrastructure as critical infrastructure to the Nation and we are directed by the President or the Secretary, I can apply our capabilities in partnership with others, because we will not be the only ones, the Department of Homeland Security, the FBI. I can apply those capabilities proactively with some of the owners of these systems.

Senator Hirono: It was very clear by General Clapper yesterday that Russia will continue these efforts. And in fact, we know that they have been doing this since the 1960s or 1970s, but it is just that they have many more tools in their toolbox to interfere with our elections. So you are still awaiting direction from the President for everyone to coordinate their efforts to stop this kind of behavior on Russia's part?

Admiral Rogers: No. I am saying I do not have a defined mission here. No one has changed that yet.

Senator Hirono: We need to do that for everybody to come together. Thank you.

The services continue to increase cybersecurity capabilities and develop advanced tools to combat cyber attacks. And PACOM has placed a focus on advanced cyber and

anti-satellite capabilities. How does CYBERCOM work with the other combatant commands like PACOM to counter the cyber threats they face?

Admiral Rogers: So I partner with -- I was just in Honolulu 2 weeks ago with Admiral Harris and his team sitting down and going, hey, because I try to get out there about -- for example, Hawaii, just an example. I am there generally every 6 months. I try to do this with all the combatant commanders everywhere around the world, sit down face to face with where are we, are we meeting your requirements.

Cyber Command in many ways -- much of what we do functions to support others. We exist to support and enable the success of others. So I always tell our team much of our success is going to be defined by others, not by us, and that is the way it should be. And so we spend a good deal of time aligning capability to meet specific combatant commander requirements, working with the combatant commanders as to what should be the priority for how those capabilities are applied. In many instances, I want them to set the priority not me. I have an opinion that we will partner together. And so, for example, that is what we are doing now in the Pacific from both a defensive and an offensive side.

Senator Hirono: And in your meetings with the other

combatant commands, then is part of your function to encourage -- to make sure that we do not have unnecessary duplication of effort across the services?

Admiral Rogers: So I try to make the argument, cyber is a high-demand/low-density capability, just like ISR, just like SOF, just like ballistic missile defense. And therefore, the same kinds of processes that we put in place to make sure we are maximizing the finite capability we have, we have got to do the exact same thing in cyber.

Senator Hirono: We know that we have challenges facing military recruiters in attempting to fill their cyber-related billets as other government agencies and the private sector try to fill their requirements as well. I would like to know specifically how important is it to continue non-military federal investments in education, particularly in the STEM programs, for American youth in order to meet the growing need of Cyber Command and other --

Admiral Rogers: Right. So as I said, our workforce is going to be a spectrum from the active, the Guard and Reserve, civilian, and contractors. For the civilian contractor and much of that active piece, much of this education is going to be done by the private sector, not by the government. So it is one reason why, as I said, we have relationships, if my memory is right, with over 200 academic institutions. It is one reason why I spend a fair amount of

time as a senior commander going to universities around the United States about so how are we going to create the human capital of the future in this. It is one reason why I spend a lot of time talking to the private sector about so tell me how you generate a workforce. How do you retain it? I acknowledge that there are some differences, but are there some things I could learn from you about what works for you? Because it cannot be all about money.

Senator Hirono: Thank you for that proactive posture. Thank you, Mr. Chairman.

Chairman McCain: Senator Tillis?

Senator Tillis: Thank you, Mr. Chair.

Admiral Rogers, it is good to see you again. You have been on the job about 2 years. Right?

Admiral Rogers: 3 years, sir.

Senator Tillis: 3.

Admiral Rogers: Yes, sir.

Senator Tillis: If you were to go back 3 years ago and you were in the same committee hearing, would the answers have changed substantially in terms of our current -- where, in other words, have we made significant progress?

Admiral Rogers: Where we made significant progress, we have capability. We are actually using it. We have got a good way ahead. We have got a commitment to that way ahead. So that is what I would have said as we --

Senator Tillis: But as you go through this, Admiral, if you think about looking at our near-peer competitors, they too are 3 years further along.

Admiral Rogers: Right.

Senator Tillis: So is the gap narrower or wider now between our capabilities to defend ourselves and to potentially respond to some attack?

Admiral Rogers: Narrowing. The gap is narrowing.

But to continue what I think was the point you are trying to make, but I would also tell myself, Rogers, you are not moving fast enough. We got to move faster. We got to prioritize. I am the first to acknowledge that. We are not where I want to be.

Senator Tillis: What about over the last 3 years, the sense of ownership in the private sector? I for one think we are making a huge mistake if we leave this hearing or if the private sector thinks we are coming up with a solution that they all benefit from. They are a part of an infrastructure that we cannot possibly be expected to -- this is sort of like, you know, we are the police, back to Senator King's point. We have to respond when an attack occurs to try and figure out who did it and what the consequences should be. But we all need to have some sort of security ourselves in our businesses, in our homes, and our States. How well have they really improved over the

last 3 years since you have been in the position?

Admiral Rogers: It is uneven by sector. Some sectors, boy, have really made significant improvements; others, no.

To go to your point, the analogy I try to use, look, it is hard to expect the police force to stop burglaries if you are going to leave every one of your doors not just unlocked but open. You are going to turn all the lights on, and you are going to leave the house for an extended period of time.

Senator Tillis: And a sign saying "not at home."

Admiral Rogers: And just say -- right -- hey, feel free. That is not going to get us where we need to be.

Senator Tillis: Well, how do we move the ball? We had TRANSCOM in here for a hearing just last week or week before. How do we actually get to a point where we put pressure on the private sector not to mandate, but to maybe use it as a distinguishing factor when we are choosing between one potential contractor or supplier and another one in terms of the extent to which we believe that they are fully protected or protected as much as they can be in this space?

Admiral Rogers: So I think it goes to a combination of we need to change the basic contract language about it and set minimum expectations if you want to do business with the DOD.

Senator Tillis: Is that within your current

authorities?

Admiral Rogers: I am sorry, sir?

Senator Tillis: Is that within current authorities?

Admiral Rogers: Yes, and we have made some across the Department. We have made some changes in contractual language, but I think the evolution has shown us we got to be more specific.

Senator Tillis: To what extent is your command trying to -- in the discussion -- I think it was with TRANSCOM -- we were talking about needing some sort of third party -- there needs to be something out there to make sure that our suppliers, maybe even State agencies, are adhering to some baseline standards. To what extent is your command involved in that or who owns that?

Admiral Rogers: So we do not do that right now, but that is one of those changes I talked about, how do we change the relationship between DOD and its core private capability providers, infrastructure providers. Perhaps one of the things contractually you look at is so if you want to do business with us, you are signing up potentially to the idea that we can do an assessment, we can do an inspection. I think we need to work our way through that, but that is the kind of thing I think we need to be thinking about.

Senator Tillis: I think it is critically important. We have to also look at the reality that they have got a

supplier base, that the people that we contract with need to make sure they are holding their supplier base up to the same standard. I will just repeat what I always say in these committees. You can find a weaker link. All you can do is understand the supply chain and go after that one critical, seemingly innocuous component that shuts down your ability to repair a grid component or to repair some weapon in the supply chain.

In my remaining time, can you tell me a -- after elevation and the dual-hat split, how do you envision a standalone command operating? And what are the priorities?

Admiral Rogers: Well, again, now we are into a kind of "what if" scenario. So I would rather not go down -- I just do not like getting into "what if" kinds of things. That decision has not been made. That is a broader policy issue. I have had the opportunity to provide input to that process, but now we need to let the process play out and see what kind of bottom line the decision-makers come to. I just think that is fair and that is what we owe them.

Senator Tillis: Thank you.

Senator Reed [presiding]: On behalf of Chairman McCain, Senator Warren, please.

Senator Warren: Thank you.

I want to quickly ask about the importance of our non-military agencies and programs to your mission, which

includes defending the United States against cyber attacks by foreign and non-state actors. Our State Department promotes international norms of responsible behavior in cyberspace, and it helps make our partners and allies more cyber secure -- I think you have already talked about that some -- and counters online radicalization and recruitment by non-state actors like ISIS every day.

So, Admiral Rogers, you lead the best cyber warriors in the world. But I want to ask, would reductions in funding to the State Department's cybersecurity and counter radicalization programs make your job easier or harder?

Admiral Rogers: Tougher.

Senator Warren: I agree. I am concerned about the significant reductions to non-DOD departments proposed by the administration. These agencies provide critical support for your work, and I just want to make sure that does not get overlooked.

What I also want to do is follow up on a question that Senator Hirono asked. Last year, the Russians stole private emails and splattered them all across the Internet to help their preferred American presidential candidate. Last week, the Russians did exactly the same thing in order to help their preferred French presidential candidate. The United States of America needs to step up its game here. And I know that you are a key part of that.

Now, you stated in your prepared testimony, Admiral, that improving DOD's network defenses and building a cybersecurity culture depend on skilled people. So I would like to press you on the question of how we recruit and retain cyber warriors. Admiral, let me see if I can do this the right way.

We had a hearing recently in our military personnel subcommittee, and one of the witnesses said that the military recruiting system is so focused on filling quotas that they end up recruiting only for the military of today, not targeting the best suited to execute the missions that we are going to need a decade from now.

So, Admiral, can you tell us about your recommendations to ensure that we are recruiting the right talent for the cyber jobs and threats that we will face tomorrow?

Admiral Rogers: So my experience to date -- knock on wood -- has been I am very happy with the quality of individuals that we are seeing.

Senator Warren: I understand.

Admiral Rogers: We are exceeding retention broadly on the uniformed side. I have got a little more concern on the civilian side actually right now in terms of retention, particularly on the NSA side of my responsibilities.

The thing that is helping us at the moment is this workforce views themselves as the digital warriors of the

21st century, and their self-image is we are on the cutting edge of something brand new and every day we are shaping the future in a way that nobody else gets to do. And we are doing things that nobody else on the outside gets to do. They are empowered by the mission. And I am not going to pretend their leadership is perfect. But my sense is they think we got a focus, we got a vision, and we are driving it.

So I am constantly as a leader looking for what are the indicators if that is changing, how do I get ahead of this, and then what are the skill sets that I need not today but maybe 2 years from now, maybe 5 years from now.

Data is one area I would highlight. I am sitting here saying to myself right now we are probably not optimized for the data requirements of the near term. So what kind of data skills do I need? Is that a uniformed skill? Do I look at civilians to do that? Would a contractor make more sense? Is that something that the Reserves could do because they can put people in a skill set, and then, boy, they are going to stay there and do that? That is probably an example of where I am saying to myself maybe we need to be looking at -- it is still in my mind. We have not developed a formal plan, so to speak.

Senator Warren: But I am glad to hear it. You are looking out. I love the focus on data, you know, critically

important here.

In the 2017 Defense Department authorization, we gave a lot of flexibility on how to recruit talent specifically. So let me just ask, do you have all the authorities you need, or do we need more exemptions, for example, from federal hiring laws and other changes in the system to help you in your recruiting efforts not just today but 6 months from today and a year from today and a few years from today?

Admiral Rogers: Well, right now I feel good about military recruitment. I find our ability to hire on the civilian side -- we are lagging. And part of this is I tell our team is this something we are failing to understand. Do we have a lack of knowledge of our own system that we are not optimizing the system to generate the outputs we need? I am not at a stage yet where I have decided the answer is I have to go ask for more authority, but I have told the team, look, if we come to the conclusion that we have to ask for more authority, guys, that is what we are doing. We have got to take advantage of the willingness of this committee, the Department to work with us when it comes to flexibility on the human capital piece.

Senator Warren: Good.

I know how much you have invested in our cyber military force and the mission force overall. You have made enormous progress. But I do hope you will let us know.

Admiral Rogers: Yes, ma'am.

Senator Warren: And let us know more in advance rather than later. It takes a little while to get things through around here. But let us know because if you need more flexibility, you should have more flexibility. Thank you, Admiral.

Admiral Rogers: Thanks.

Chairman McCain [presiding]: Senator Perdue?

Senator Perdue: Thank you, Mr. Chair.

Admiral, good to see you again. Thank you for everything.

In testimony we heard earlier this year, the Defense Science Board said -- and I quote -- for at least the next decade, offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructures. Do you agree with that from the Defense Science Board?

Admiral Rogers: I said broadly. Clearly things favor the offensive side. Part of our challenge is much of our infrastructure represents investments and decisions and priorities made decades ago, and they are not reflective of the digital world we find ourselves in today. And the cost of replacing that fixed infrastructure is huge. And so it is not likely that we are going to replace all of that infrastructure in the immediate near term. Just the scale

is just beyond the ability of our society or our Nation right now.

Senator Perdue: So we are primarily focused on defense, deterrence, and detection right now from your earlier testimony, even today in this written testimony. My question is, in an open hearing like this, is there anything you can tell us about what we are doing on the offensive side? Are we developing offensive capabilities as well?

Admiral Rogers: So we have acknowledged that we are developing offensive capabilities. We have acknowledged that we are employing those capabilities in the fight against ISIS. I apologize. I would just rather not get into the specifics.

Senator Perdue: I understand.

I would like to move over to the question of the day, and it is how do you stand up this force over the next few years. And training is a very major part of this, as you have said. Between 2013 and 2016, under CYBERCOM's supervision, the Office of the Secretary of Defense and the Joint Staff were supposed to come to an agreement on a joint federated training program funded by the services for the training of the Cyber Mission Force. Can you update us on the status of that agreement and where we stand today on that?

Admiral Rogers: So we will transition to that model in

2018. The initial outfit, if you will, of the Cyber Mission Force, using much of NSA's infrastructure -- we signed up, speaking now as the Director of NSA, to use much of NSA's structure, our schoolhouses, our National Cryptologic School, for ex4ample, to do much, not all, but to do much of the training associated with the initial build-out of the mission force. That build-out, full operating capability is due to be completed, and we are on track for 30 September 2018. The agreement then was at that point responsibility for training and development, long-term sustainment of the force would transition to a service structure. We are on track to do that right now.

Senator Perdue: So does that mean that each service would be responsible for developing their own cyber warriors?

Admiral Rogers: So what happens is we have a mandated training standard by position, each service then oftentimes partnering. For example, right now there is Navy training in Pensacola that all the services use, for example, because we all then get together and say so given this single common standard, given this single, agreed-to qualification process, what is the best way across the Department to make this work. What service has the best capacity, best capability? How do we manage throughput broadly? That is the only way to maximize this.

Senator Perdue: You mentioned context earlier, which is why you do not favor a unified force.

Admiral Rogers: Right. I was thinking about an integrated cyber --

Senator Perdue: I understand. I get it.

So having some experience in large organizations, I am concerned about that tradeoff. There is a balance.

Admiral Rogers: Right. Yes, sir.

Senator Perdue: We are in a crisis stage right now -- I think you would agree to that -- with regard to our ability to detect and deter at this point. I understand long-term the ideal might be to have the service because of the context dimension.

In the interim phase when we are in this crisis mode, though, do we have a sense that that might be counterproductive to our ability to stand up to the immediate threats?

Admiral Rogers: It would be difficult to do it today in a short term. That would take a long-term investment, significant structural, cultural changes. It is another reason why I would argue optimize the structures and the mechanisms that are in place. Now, we also got to hold them accountable. Do not get me wrong. You just cannot turn to them and say, well, just do what you always do. There has to be accountability and oversight.

But I am comfortable that the current approach is going to generate the outcomes we need, even as I acknowledge it is not moving as fast as I would like. And we got a huge mismatch between current capacity and capability, and what I know is the requirement. We are always in a tail chase.

Senator Perdue: You mentioned earlier that the history has been the extraction of data from the system, that hacking -- the primary motive from Russia and China, primarily state actors, has been the extraction of data.

In North Korea, we saw a little bit of a different attack where they went in and actually started placing what I would call a sleeper embedded code, whatever, for a bigger mega event later. Do we see a continuing growth in that type of activity? Have we seen any evidence of that in the U.S.?

Admiral Rogers: You do. You see every nation state engaged. They will penetrate a system. They will look to not just extract but study it, understand it, see where it connects to. Can they use this as a jumping off point to get to somewhere else?

One of the things we are always looking for is so if a system has been penetrated, has the actor manipulated, changed, amended a configuration so they can gain access separately now. That is one of the key things we always look for when we are trying to do mitigation once someone

has penetrated a system.

So it is the full spectrum. The simple answer is yes. It is the full spectrum.

Senator Perdue: Have we seen any in the U.S., any evidence of that in the U.S.?

Admiral Rogers: I have seen nation states engaged in activity in the U.S. where they clearly are interested in a long-term presence, not just extracting data.

Senator Perdue: Thank you, Admiral.

Chairman McCain: Senator Peters?

Senator Peters: Thank you, Mr. Chairman.

And, Admiral Rogers, always a pleasure to see you and enjoy your testimony as always.

My question involves the U.S. semiconductor industry, which right now faces some major challenges. In addition to some fundamental technological limits that are being reached in that area, there has also been a concerted strategic push by China to reshape the market in its favor using industrial policies backed by over $100 billion in government-directed funds. And with semiconductor technology critical to the operation of critical U.S. defense systems, I am very concerned that China's industrial policies pose a real threat to U.S. national security.

And although we have a range of tools, which you are very familiar with, to deal with this, the principal

mechanism to manage it is the interagency Committee on Foreign Investment in the U.S., or CFIUS. And within the DOD, as you know as well, NSA is a key contributor to the CFIUS national security assessment. DIA, the military services, the combat commands all have a role in this process as well.

But my question is considering CYBERCOM's leading role within the Department, how is the command postured to support the CFIUS process for potential foreign mergers and acquisitions that have perhaps significant implications for the DOD cyber mission?

Admiral Rogers: So we predominantly interact in the CFIUS process on the NSA side. But one of the implications I think for the future -- again, it is just one input I have tried to make to the new team is I think we need to step back and reassess the CFIUS process and make sure it is optimized for the world of today and tomorrow because I am watching nation states generate inside knowledge about our processes. They understand our CFIUS structure. They understand the criteria broadly that we use to make broader policy decisions about is an investment acceptable from a national security perspective. And my concern is you are watching some nation states change their methodology to try to get around this process.

Senator Peters: Do you feel that CFIUS is adequately

resourced and authorized to make the kinds of changes that you think we need --

Admiral Rogers: I am not smart enough because we are just one element in this process, and it is not something that the DOD at large or Cyber Command or NSA runs per se. But I do think we need to step back and ask that kind of question to ourselves. Just my gut just tells me that that is one of the things we need to be doing.

Senator Peters: I would like to turn back to some of the discussions that we have had related to the involvement of the private sector, which has to be intimately involved in any kind of security operations. And I know your teams have operated Cyber Guards, over the years, exercises. And the most recent on you were involved in, simulating an attack on the Northeast, attacks on gulf oil facilities, ports across California. All of these entities, of course, are privately owned and not part of the Department of Defense.

And a recent GAO study, looking at some of the prior exercises, cited concerns that large portions of the exercise take place in a classified forum which places some inherent limitations on public and private sector participation. And although the arrangement certainly is designed to protect sensitive plans and capabilities -- and we all fully realize the importance of doing that -- the

approach also may fall short in preparing participants for a real world cyber emergency, which potentially could be catastrophic.

So my question is, how are you balancing the need for security with the realities of a cyber threat landscape that may ultimately necessitate very broad support from uncleared citizens and entities?

Admiral Rogers: So it is one of the reasons we changed the structure of Cyber Guard over time and tried to bring more in the private sector. So if you look at the scenario that you talked about that we did last year in terms of we simulated activity directed against the power grid in the east, the petroleum industry in the gulf, and port sectors on the west coast. We went to several private companies within each of those sectors and said, hey, we would like you to participate in this. What do we need to make that happen?

We also increasingly are going to the private sector in terms of private sector companies that run the infrastructure associated with supporting those entities. We have added that to the Cyber Guard arena.

So I am trying to see can we create an exercise in addition. We do tabletop exercises, which are not quite -- Cyber Guard is huge. It is like a thousand individuals.

We also do regular tabletop exercises where we talk at

a high level so we can skirt some of the security aspects of the classification aspects of this and bring in the private sector. We do that out at the Fort Meade complex several times a year separately from Cyber Guard.

Senator Peters: Thank you, Admiral.

Chairman McCain: Senator Cotton?

Senator Cotton: Thank you, Admiral Rogers. Welcome back.

I want to talk about Russia today and how they hacked into those emails and released them last year. I want to touch on that.

Specifically Senator Warren a few moments ago continued to refer to the President as Russia's preferred candidate. I think she is referring there to the intelligence community assessment of January 6th, primarily written by your agency, the NSA, along with the CIA and the FBI.

This brings to mind a curiosity from the report that I wanted to raise with you and ask about. In the key judgments, the report says we also assess Putin and the Russian Government aspired to help President-elect Trump's election chances, when possible, by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment. NSA has moderate confidence.

Could you explain the discrepancy for us?

Admiral Rogers: I would not call it a discrepancy. I would call it an honest difference of opinion between three different organizations. And in the end, I made that call. So if anybody is unhappy, Mike Rogers is the accountable individual.

When I looked at all the data, I was struck by for every other key judgment in the report by multiple sources, multiple disciplines, and I was able to remove almost every other alternative rationale I could come up with in my mind for, well, could there be another reason to explain this. In the case of that one particular point, it did not have the same level of sourcing and the same level of multiple sources from different perspectives, you know, human intelligence, signals intelligence.

I still believe that it made sense. I still believe that it fit within the context, and I still agreed with the judgment. But I did say from a professional analytic perspective, I am not quite at the same confidence level as my two counterparts in the form of John Brennan and Jim Comey.

Senator Cotton: The one particular point being going from saying Russia wanted to hurt Secretary Clinton's chances, in addition help Donald Trump's chances.

Admiral Rogers: Correct.

Senator Cotton: Those are hard to disentangle -- right-- since in our election system we have to first pass the post as long as you do not have a --

Admiral Rogers: In this case, there was some pretty specific intelligence that seemed to differentiate that there were specific thoughts on the part of the Russians on each of the aspects of that statement, if you will.

Senator Cotton: Obviously, we cannot discuss those classified matters, but there is a lot of open source matters as well. President Trump, for instance, was the candidate who wanted to build up our defenses, expand our missile defenses, accelerate nuclear modernization, pump more North American oil and gas. None of those things seemed to be very favorable to the Kremlin. Did your agency take those things into account?

Admiral Rogers: Yes, sir.

Senator Cotton: And also if you look back over the last 8 years, just a quick rundown of what I could recall -- I am sure I am missing some -- the Obama administration in 2009 reset relations with Russia 6 months after it invaded Georgia.

2010, signed New START, which I would say was a better treaty for Russia than us.

2012, in a hot mike moment with Dmitry Medvedev, President Obama said he would have more flexibility on

ballistic missile defense after his election. He also mocked his opponent at a presidential debate saying that Russia as our number one geopolitical foe.

2013 was the red line fiasco in Syria with Russia's closest Middle East ally when President Obama accepted Vladimir Putin's offer to remove chemical weapons from Syria, which we now know was a failed effort.

2014, we stood largely idly by during the Crimea invasion and did not offer defensive weapons when Russian-backed separatists started fighting in the Donbass despite bipartisan support from this committee. By that point, we had long since been ignoring INF Treaty violations that our military now acknowledges.

2015, Russia had a massive surge into Syria and continued its effort to block U.N. Security Council resolutions.

2016, they pummeled Aleppo into submission. In private, they objected to numerous provisions that I wrote in the Intelligence Authorization Act that would hold Russia to account in its espionage effort, and they increased the amount of times they are buzzing aircraft and warships in Europe and the Arctic.

President Trump promised to reverse those policies. Secretary Clinton largely campaigned on continuity. That does not sound to me like something that the Kremlin would

be happy about.

Admiral Rogers: I am just going by the intelligence. It was very clear in the intelligence of Russians' perceptions.

Senator Cotton: Do you think given that 8-year history of the Obama administration that Russian intelligence and leadership felt emboldened to undertake the hacks of those email systems and release them?

Admiral Rogers: Now you are into political judgment, sir, and that is just not my area.

Senator Cotton: Thank you very much.

Chairman McCain: Senator Kaine?

Senator Kaine: Thank you, Mr. Chair.

Just to follow up, Admiral Rogers, on this issue of moderate confidence, did you have a high degree of confidence that there was an effort to discredit one candidate and only a moderate degree of confidence that there was an effort to support --

Admiral Rogers: If you read the key judgments, what it says is I concurred in the report in the sense that we had high confidence in the judgment that the Russians clearly were trying to undermine our democracy and discredit us broadly, that they wanted to specifically make sure candidate Clinton did not win and to undercut her effectiveness should she have won.

Senator Kaine: High confidence in that.

Admiral Rogers: Right. High confidence in that and that it was just the last part about -- and their judgment was they wanted candidate Trump to win. And that was one of the objectives --

Senator Kaine: We had testimony in this committee probably a year and a half ago by General Dunford where he was asked the question I think by Senator Manchin which was the nation state that he would view as our most significant adversary. And he testified, based on their capacity and intent, he thought that would be Russia.

Just in your domain, cyber, the cyber domain, do you view Russia as an adversary? They have taken actions that have put them in the position as an adversary of the United States in the cyber domain.

Admiral Rogers: I am watching them engage in behaviors that I think are destabilizing and not in our best interests in cyber.

Senator Kaine: Would you also agree that France is an ally? They are a NATO ally and they are also a coalition partner in Afghanistan.

Admiral Rogers: Yes, sir.

Senator Kaine: You are aware of the reports in the last few days that there was significant evidence tying Russia to a hacking effort to destabilize the French

election. That is something we should take seriously when an adversary tries to destabilize the government of an ally. Would you agree?

Admiral Rogers: Yes, sir.

Senator Kaine: There was an article in the "New York Times" the day before the election, Saturday, the 6th, with a fascinating headline. "U.S. Far Right Activists Promote Hacking Attack Against Macron," and the article was about the effort by groups in the United States to immediate spread the hacked documents in many instances before even WikiLeaks was able to.

If we should take seriously an adversary's cyber attack on the democracy of an ally, should we be indifferent or concerned about efforts of Americans to work together with or in parallel with an adversary attacking the democracy of an ally?

Admiral Rogers: I apologize. I am not sure I am understanding.

Senator Kaine: You have testified in response to my question that we ought to take seriously if an adversary tries to cyber attack and destabilize the democracy of an ally. If American organizations are working together with or in parallel with an adversary --

Admiral Rogers: A foreign counterpart?

Senator Kaine: -- as they are trying to attack the

government of an ally France, should we be in different to that, or should we take that seriously as well?

Admiral Rogers: We need to be concerned.

Senator Kaine: Okay. And if we are concerned about that, if the U.S. Government should be concerned in this case -- and I will introduce this article for the record.

[The information follows:]

[COMMITTEE INSERT]

Senator Kaine: If we should be concerned about the efforts of folks in the United States to work together with or in parallel with an adversary like Russia attacking an ally like France, where should that concern lie in the Federal Government? Is that a law enforcement matter? Is it a DHS matter? Is it an NSA matter, or is it a Cyber Command matter?

Admiral Rogers: I would argue it depends on the specifics of the scenario. I am not trying to be dismissive, Senator. It is a very complex question.

Senator Kaine: And I will put the article in for the record, and there is, I think, more to come on this.

But if individuals or organizations in the United States, for example, were taking hacked documents from an illegal Russian hack of the French system and trying to disseminate it to affect the French election, this is something we should be concerned about. Where would that concern lie within --

Admiral Rogers: My first thought would be the FBI, but again, that is not necessarily a fully informed opinion, but it is the first thing that comes to my mind.

Senator Kaine: All right.

Let me ask you this. There has been some debate in the last couple of days about whether there is such a thing as a good shutdown of the United States Government. Can you see

any circumstance under which Cyber Command's mission would be benefited by a shutdown of the Government of the United States?

Admiral Rogers: No. And if I could, I know you are asking for a yes or no. The number one issue that my workforce often raises with me is what we went through in 2013, and it is now 4 years later. And I still -- every time there is the merest hint in the media of this even potentiality, I get, sir, are we going to go through this again, sir? You said this was not going to happen, sir. I thought they were committed to us and our mission. Sir, I do not want to work in an environment where every couple of years I am just getting jerked around about am I going to come to work, am I going to get paid, do they value what I do. Hey, sir, we just want to do the mission. We just need the support to keep moving forward.

Senator Kaine: Thank you, Admiral.

Thank you, Mr. Chairman.

Chairman McCain: Senator Graham?

Senator Graham: Thank you, Admiral. Thank you for your service.

Director Comey said a couple of days ago -- I guess it was last week in the hearing that I was involved in in Judiciary -- that Russia is still interfering in American politics. Do you concur with that?

Admiral Rogers: Yes.

Senator Graham: He also said that among nation states, he thought Russia had the most capability and the biggest intent in terms of interfering in the future. Do you agree with that?

Admiral Rogers: Yes.

Senator Graham: Do you agree that it was Democrats in 2016? It could be Republicans in the next election?

Admiral Rogers: Yes. I would argue this is not about politics. This is not about party. This is about an effort against the strategic interests of every citizen of this Nation.

Senator Graham: I agree with you 1,000 percent.

Do you they agree they could do this in congressional races, House and Senate --

Admiral Rogers: Yes.

Senator Graham: Do you agree that if somebody does not make them pay a price, they are going to keep doing this?

Admiral Rogers: Yes.

Senator Graham: All right. Unmasking. A lot of talk about it. Are you aware of any incidental collection on 2016 candidates on both sides of the aisle?

Admiral Rogers: I am not going to get into specifics in an unclassified forum about collection at large. But I will say we certainly acknowledge that incidental collection

occurs, but we also have a very strict process --

Senator Graham: Can we build that out a bit?

Admiral Rogers: -- for what we do with it.

Yes, sir.

Senator Graham: The only way you can actually collect on an American citizen inside the country is to have a FISA warrant.

Admiral Rogers: Get a FISA warrant. Yes, sir.

Senator Graham: Or if an American citizen is incidentally in a conversation with somebody you are already following.

Admiral Rogers: Yes, sir.

Senator Graham: Unmasking is a request to your organization, I want to know who American citizen 1 was.

Admiral Rogers: Yes, sir.

Senator Graham: How many of those requests did you get in 2016?

Admiral Rogers: I think we have publicly acknowledged --

Senator Graham: Around 2,000.

Admiral Rogers: 2,000. I think it is --

Senator Graham: How many people can request the unmasking of American citizens?

Admiral Rogers: If you are an authorized recipient of the intelligence, we use two criteria. Number one, the

requester must be asking this in the execution of their official duties. It cannot be something that would be need to know. Number one has to be in the execution of their official duties. Number two, the revealing of a U.S. person has to provide context and greater value for the intelligence. Again, it just cannot be I am just curious.

Senator Graham: I got you.

So within our government, are there 10 people -- 10 groups that groups that can do this? 20?

Admiral Rogers: In terms of authorizing the unmasking?

Senator Graham: Yes. No, to make the request.

Admiral Rogers: No, it is broader than that. If you are on the distribution -- if you are on the authorized distribution for our intelligence reporting, you can ask. It does not mean it gets approved, but you can ask.

Senator Graham: Does the National security Director -- one of those -- I mean --

Admiral Rogers: The National Security Advisor? Yes, sir. They are normally on the distribution for most, not all.

Senator Graham: Is there a record of every request made?

Admiral Rogers: Yes.

Senator Graham: So there is a record of who made the request to unmask the conversation involving the American

citizen.

Admiral Rogers: Yes, sir.

Senator Graham: There is a record whether or not you granted it.

Admiral Rogers: Yes, sir.

Senator Graham: Is there a record of what the person did with the information once they got it?

Admiral Rogers: No. There is also a record of the basis of, so why did we say yes. Remind every individual, if I could, once we unmask, once we authorize an unmasking, we authorize the unmasking only to that individual. What do I mean by that? So if we unmask a report that went to a particular individual, we do not unmask the report for everyone who got that report. Only the individual that we --

Senator Graham: And they are told not to share it with --

Admiral Rogers: And they are specifically told. This does not change the classification.

Senator Graham: General Flynn was caught up in a conversation with the Russian ambassador. You are familiar with that story in the press.

Admiral Rogers: I am familiar with the story. Yes, sir.

Senator Graham: Assuming he did not have a FISA

warrant allowing us to collect on him, it would be a case of incidental collection following the Russian ambassador. Does that sense?

Admiral Rogers: Yes, sir.

Senator Graham: We would know how that conversation was revealed and to who it was revealed through the request of your agency.

Admiral Rogers: If we unmasked and it was based on an NSA report. Remember, NSA will not be the only agency that potentially could have gotten the conversation.

Senator Graham: Got you, but you are the primary one. Right?

Admiral Rogers: I would argue again it depends. If you look at Title 1 warrants, the FBI --

Senator Graham: I am not talking about warrants. I am talking about --

Admiral Rogers: Incidental. So I would argue there is probably a greater potential on the FBI side than NSA just generally in terms of collection.

Senator Graham: Of incidental collection?

Admiral Rogers: Incidental with U.S. persons.

Senator Graham: So we could either ask the FBI or you.

Admiral Rogers: Yes, sir.

Senator Graham: So somebody took that information that we gained through collection with Flynn and gave it to the

"Washington Post."

Admiral Rogers: Somehow it got to the media.

Senator Graham: That is a crime.

Admiral Rogers: And that is a leak, and that is illegal. Yes, sir.

Senator Graham: Are you concerned about people taking the law in their own hands no matter how noble they think the event would be?

Admiral Rogers: Oh, yes, sir, which is why I have gone to my workforce in writing and said let us make sure we understand what the professional ethos of our organization is. We do not -- if I could finish, sir. We do not engage in this behavior, and if I catch you engaging in this behavior, I will hold you criminally liable and you have no place --

Senator Graham: Mr. Chairman, can I ask for additional 30 additional seconds?

The bottom line here, it is possible for the Congress to find out who requested unmasking of American citizens, who that information was given to, and that is possible for us to know.

Admiral Rogers: On the NSA side, that is part of the ongoing investigation with the primary oversight committees that we are going through right now.

Senator Graham: Do you know is Susan Rice ever asked

for an American citizen to be unmasked?

Admiral Rogers: I would have to pull the data, sir. I apologize.

Senator Graham: Thank you.

Chairman McCain: Senator Blumenthal?

Senator Blumenthal: Thanks, Mr. Chairman.

Thank you, Admiral Rogers, for being here again and thank you for your service.

We have heard repeatedly in this room, as well as yesterday with Director Clapper, that the Russians will continue attacking the United States unless they are forced to pay a price. And you agree.

Admiral Rogers: Yes, sir.

Senator Blumenthal: And right now, are they being forced to pay a price?

Admiral Rogers: Certainly nothing that is changing their behavior.

Senator Blumenthal: Nothing that is changing their behavior, and clearly nothing that will change their behavior in the future because, to quote you or paraphrase you, they have more to gain than to lose by continuing this kind of attack.

Admiral Rogers: Yes, sir.

Senator Blumenthal: So can you recommend to us what kinds of measures should be taken? And I know you have been

asked this question before. In fact, you were asked when you last testified here. And you said that tools like sanctions can be an effective option. But so far, the sanctions in my view are way less than they should be. Do you agree that sanctions can and should be increased to provide a price that the Russians --

Admiral Rogers: So now you are into a policy judgment. I will only say sanctions I think have proven to be an effective tool in many scenarios. I am not going to argue that they are perfect and they work all the time.

Senator Blumenthal: But there will be a point where a cyber response should be appropriate.

Admiral Rogers: Potentially although I would highlight when we think about deterrence, we need to think more broadly than just cyber. Just because someone comes at us in cyber, does not mean we should automatically default to, well, it has got to be an exact response in kind. I think we need to think more broadly and play to our broader strengths as a Nation.

Senator Blumenthal: There is no question that the Russians attacked this country through cyber. And would you agree that Americans who colluded or cooperated with that attack also should be held accountable?

Admiral Rogers: Broadly yes, but again, now you are starting to get into a legal and a policy piece, and that is

just not my lane in the road.

Senator Blumenthal: Well, your lane includes defending this Nation from cyber attack.

Admiral Rogers: Yes, sir. But not necessarily action against particular individuals.

Senator Blumenthal: Well, let us talk about a group of Americans who may have colluded or cooperated with the Russians in enabling or encouraging this kind of attack. And by the way, they violated criminal laws if they did so. Would you not agree that they should be held accountable and that an investigation of it is appropriate and necessary?

Admiral Rogers: So I agree an investigation is appropriate and necessary, and if they violated the law, then, yes, sir. I am just not an attorney. I am not a lawyer. I am not a law enforcement individual. It is not my area of expertise.

Senator Blumenthal: But unless they are made to pay a price as well, the Russians will be enabled and encouraged in the future.

Admiral Rogers: Yes, sir.

Senator Blumenthal: And they will be paying less of a price as well.

Admiral Rogers: Right.

Senator Blumenthal: I feel like we are in a time warp here because when you were last here, we agreed that we need

a policy and a strategy, as the chairman has articulated so well, and we still do not have one. Can you tell the American people whose responsibility it is to develop that strategy and policy?

Admiral Rogers: It is ultimately the executive branch. There are multiple components, but ultimately it boils down to the executive branch. As I have said, look, we have a new team in place. They are working their way through this. In fairness to them, this is not a -- this is a complicated topic with a whole lot of complexity and nuance. I know that these discussions are ongoing. I have been a part of some of them. I am grateful that the team is willing to reach out and say, hey, Admiral Rogers, from your perspective, what do you think, what do you see, what are you thinking about. So I do not want anybody walking away thinking nothing is going on, no one is thinking, they are not attempting to proactively try to grapple with these very tough problems.

Senator Blumenthal: Well, I just want to conclude by stressing again that forcing the Russians to pay a price for their attack on this country requires compelling Americans who colluded or cooperated with them to pay a price, but also a strategy and policy for knowing when there is a cyber attack on this Nation, when it is an act of war that should prompt a response in the cyber domain or in other military

domains and economic sanctions that also may force them to pay a price. And right now, our policy of deterrence is in my view an abject failure.

Admiral Rogers: Not achieving the desired result. That is clearly true. Yes, sir.

Senator Blumenthal: Thank you.

Thanks, Mr. Chairman.

Chairman McCain: Senator McCaskill?

Senator McCaskill: Thank you, Mr. Chairman.

Good to see you, Admiral. Thank you for your service.

We have heard over and over again in multiple hearings-- and we have got our cyber hearing in Homeland Security tomorrow. So this is really timely for me -- about poor information sharing and understanding the challenges of classified information.

My staff has tried to chart the national cybersecurity structure for me. And the one thing that sticks out to me is this cyber unified coordinated group. It appears to me to be really the only place that our structure is set up under PPD-41 where the private sector entities really seem to plug into the national structure. The interesting thing is this cyber unified coordinated group is supposed to be in response to a significant cyber event. That is the operative phrase.

In the United Kingdom, the NCSC has real-time

collaboration with emphasis on exchange of classified information on an ongoing basis.

My first question for you is has the cyber unified coordinated group ever been called into a session. Has there ever been ongoing meetings? Have there been any meetings of this particular group that is laid out in PPD-41?

Admiral Rogers: It does interact. It does operate. I would be the first to admit, ma'am, I have to take the question for the record about has it ever physically met.

We participated in it, and I am trying to remember if it is done. Some of the work we do virtually. We will take an issue and we will do it via email and video conference. If I could, if you would like, I can take that for the record.

[The information follows:]

[COMMITTEE INSERT:}

Senator McCaskill: Yes, because I am trying to think. It seems to me like to me the Russian thing is a significant cyber event. And I guess my problem is with this, I know we have spent a lot of time today struggling about what our policy is. It looks like to me that we do not really have anywhere where there is an ongoing meeting structure that integrates the private sector into what is a pretty convoluted setup that we have right now.

Admiral Rogers: Could I disagree slightly, if I could?

Senator McCaskill: Sure.

Admiral Rogers: I think it is fair to say that at a sector level we do have constructs that enable that to occur. But one of the things the hack points out -- for example, the Russian influence effort points out is we do not have a sector labeled U.S. election infrastructure like we do in power, like we do in transportation.

Senator McCaskill: Although DHS has named election infrastructure as part of their critical infrastructure --

Admiral Rogers: Right, now.

Senator McCaskill: -- responsibility.

Admiral Rogers: Yes, ma'am. Now.

Senator McCaskill: And that happened last year maybe in response to this. I hopefully will find out more tomorrow.

I guess it seems to me that when someone is impacting

our elections, that overlooks all because if you look at this list, our national policies certainly impact chemical, commercial, communications, manufacturing, dams, I mean everything gets impacted.

Admiral Rogers: Right.

Senator McCaskill: Forget about Russia for a minute. Are you familiar with the UK model?

Admiral Rogers: Yes, ma'am, very much so.

Senator McCaskill: So why are we not doing that? What is wrong with it and why are we not emulating it more?

Admiral Rogers: So, first, let us look at what the UK model is. They basically -- I am going to paint a simplistic picture. They turned to their intelligence structure, in this case, GCHQ, which NSA's equivalent. They turned to GCHQ and said you have the preponderance of capability, insight, expertise. We would like you to take a portion of that capability, and we are going to create this National Cyber Security Centre. In fact, the individual who runs it, a guy I have worked with for a long time, is a GCHQ employee. They decided that in their construct they were comfortable with that.

For us on the U.S. side, we have always been less comfortable with the idea of, well, do you want the intelligence world to be the primary interface, if you will, with the private sector. For our UK teammates, they are

just very comfortable with that. And their view is it is about aligning the greatest expertise and capability with the private sector, and there is not quite the same baggage or at least history or tradition.

Because of that, on the U.S. side, we have taken a very fundamental different approach, I am hoping with this new team coming in, this is opportunity for us to step back and say to ourselves are we happy with the way this is working. I have not seen your diagram, but you have heard me say for a long time we have got to simplify the complexity of this structure to the outside world because if you are in the private sector and you are trying to figure out so who am I supposed to be dealing with and why this time was it you and the last time it was that organization and the next time you are telling me you want me to go there. We have got to simplify this.

Senator McCaskill: Well, I am down for that. And I think the curse and the blessing is how protective we are of classified information. And I understand that challenge. But boy, oh, boy, pulling this group together after a significant cyber event, there is going to be a lot of Monday morning quarterbacking over whether or not more information should have been shared.

Admiral Rogers: If I could also make one point. I agree with everything you said, but I would remind people

perfect information sharing in terms of classified in and of itself will not necessarily fix every problem. If you look at reactions to the Russian hack, there were plenty of organizations that were provided the specific insights who just opted, for a variety of reasons, not to react in the same way. And that was not about classification. So I just want to make people -- I just want us to think us to think about, hey, this is the simple cure-all.

Senator McCaskill: I get it.

Admiral Rogers: And I am not trying to say that you are painting that, ma'am.

Senator McCaskill: No. I know it is not the simple cure, but I know that that underlying disease about information sharing goes deep and it is calcified. And I want to make sure that we are aware of that.

Admiral Rogers: Yes, Senator.

Senator McCaskill: Thank you, Admiral.

Senator Reed [presiding]: On behalf of Chairman McCain, Senator Shaheen, please.

Senator Shaheen: Thank you, Mr. Chairman.

And thank you, Admiral, for being here and for the job that you do.

And just to pick up a little bit on Senator McCaskill and the issue of classified versus unclassified, the challenge with, in this case, the Russian hack with so much

of the information being classified is that the American public does not know what is going on. And when the American public does not know what is going on on an event of this magnitude, that is a real challenge for our democracy.

And I was not able to hear your testimony and the questions, obviously, because I was in another hearing. But I know that there have been a number of questions about the Russian hacking and what that means. But have you talked about what in the big picture that means? What is Russia really trying to do with the hack of our electoral system, with the hack of France, with the interference in Germany, with what they have done in many of the Balkan countries, in Eastern Europe? What is their goal?

Admiral Rogers: Well, I am going to talk about the U.S. side and then talk about it more broadly.

So on the U.S. side, as we indicated, speaking to you now as the Director of NSA, as we said in the intelligence community assessment, three primary goals we thought.

First was to undercut the United States and its broad principles of democracy and try to send a message, hey, look, these guys are every bit as inconsistent as everybody else. They are not this high-on-the-hill, perfectly white and perfect structure. Look, they have pettiness. They work against each other. So to undercut our democracy.

Secondly, they clearly had a preference that candidate Clinton not win, and they also wanted to ensure if she did win, that she was weakened.

And then the report talks about the third objective was to try -- and this is where NSA has a difference confidence level than my other teammates. But I agree with the judgment that the third objective was to help candidate Trump win. If you look at the activity they have done in the United States, if you look at the activity they have done in France, in Germany, they clearly are trying to help ensure that leaders they believe might be more inclined -- it does not mean that they necessarily are, but the Russians appear to be assessing that some leaders might be more inclined to be supportive of their positions, their views, might engage in policies more favorable from a Russian perspective. You saw that just play out in the French election where there clearly was a difference between these two candidates and their views of Russia and the things they were talking in the campaign about if they won, what would some of their choices be in terms of national security policies for France and how that might impact the Russians.

Senator Shaheen: But is the overarching strategy not not so much who the winners and losers are, but it is to undermine the public confidence in a democracy and how it works?

Admiral Rogers: That is why I say that is a part of it. I am sorry if I did not make that jump on the foreign side as well. It is the same thing. That is an aspect of it.

Senator Shaheen: Right. So just as they are engaging in a military buildup, just as they are engaging in the cyber intrusions, that the other thing they are engaging in is an effort to undermine Western democracies. That is another way they are going to undermine the West.

Admiral Rogers: Right, to weaken them, to forestall their ability to respond because there is no political consensus because they distrust their institutions as citizens, et cetera. Yes, ma'am.

Senator Shaheen: So I was in Poland after the Munich Security Conference and met with a number of officials there. And some of the people that we met with suggested that they were very concerned that we had not responded to the Russian attack of our election system. And one of the things that really impressed me was the person who said, you know, if you are not willing to do anything about what Russia did in the United States intervening in your electoral system, fundamental to your democracy, how should we have any confidence that you will defend us when the Russians come after us.

So what does it say to our allies that we have not been

willing to take any overarching action against Russia for what they did? We have not been willing to pass stronger sanctions. We have not been willing to do other efforts to take action against them because of their interference. What does that say to our allies?

Admiral Rogers: So I can certainly understand why our allies would be perplexed. If this conduct occurred, why are we not seeing X, Y, or Z? I certainly can understand that.

One of the things we try to assure our allies, though, is this is one aspect of a broader set of issues. You should not question -- it depends on the relationship, but in broad terms, you should not call into question our long-term commitment to you, for Poland, for example. Do not let there be any doubt of that.

Senator Shaheen: So we are more committed to Poland than we are to addressing Russia's --

Admiral Rogers: That is not what I said.

Senator Shaheen: I know it is not what you said. But it leaves open to interpretation that assumption. So thank you.

Admiral Rogers: Yes, ma'am.

Senator Reed: Thank you.

Admiral Rogers, thank you for your testimony today. As always, we appreciate your service, and would you

communicate to your colleagues our appreciation for their service also?

On behalf of Chairman McCain, the hearing is adjourned.

[Whereupon, at 11:48 a.m., the hearing was adjourned.]

STATEMENT OF

ADMIRAL MICHAEL S. ROGERS

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

SENATE COMMITTEE ON ARMED SERVICES

9 MAY 2017

Chairman McCain, Ranking Member Reed, and Members of the Committee, thank you for your enduring support and the opportunity today to represent the hard-working men and women of United States Cyber Command (USCYBERCOM). I welcome the opportunity to describe how USCYBERCOM leads Department of Defense (DoD) efforts in the cyberspace domain and supports the nation's defense against sophisticated and powerful adversaries.

The Department of Defense recognized seven years ago that the nation needed a military command focused on cyberspace. USCYBERCOM and its subordinate elements have been given the responsibility to direct, operate, and secure the Department's systems and networks, which are fundamental to the execution of all DoD missions. The Department and the nation also rely on us to build ready cyber forces and to be prepared to employ them when significant cyber-attacks against the nation require DoD support.

USCYBERCOM has been a sub-unified command under U.S. Strategic Command (USSTRATCOM) since its creation in 2010. The command includes six operational-level headquarter elements, assisted by U.S. Coast Guard Cyber, a component of the Department of Homeland Security (DHS). USCYBERCOM's action arm is the Cyber Mission Force (CMF), which comprises 133 teams and is continuing to build to a total of approximately 6,200 military and civilian personnel. All of those CMF teams reached at least initial operational capability in 2016. Many have attained full operational capability (FOC), and I expect all of them will attain FOC status by 1 October 2018, just 15 months from now.

I want to update you on our initiatives and plans for that time to come. Our three lines of operations are to provide mission assurance for DoD operations and defend the Department of Defense information environment; to support joint force commander objectives globally; and to deter or defeat strategic threats to U.S. interests and critical infrastructure. We conduct full spectrum military cyberspace operations to enable actions in all domains, ensure US and Allied freedom of action in cyberspace, and deny the same to our adversaries. I have asked that our Command and its components focus their efforts in several areas to ensure we can accomplish missions, both now and in the future. Defense of DoD information networks remains our top priority, of course, and will move this beyond a network focus to one that includes weapon systems/platforms and data. We will also continue progress on the CMF build and attainment of FOC for all teams, while increasing the CMF's readiness and its ability to hold targets at risk. We will posture the CMF to deliver effects across all phases of operations; to improve operational outcomes by increasing resilience, speed, agility, and precision; to generate operational outcomes that support DoD strategy and priorities; to create a model for successful Reserve and National Guard integration in cyberspace operations; and finally to strengthen partnerships across the government, with our allies, and with the private sector.

Your strong and continuing support is critical to the success of the Department in defending our national security interests, especially as we comply with the recent National Defense Authorization Act directive to elevate USCYBERCOM to unified combatant command status. As you well know, I serve as both Commander of USCYBERCOM and Director of the National Security Agency and Chief, Central Security Service (NSA/CSS). This "dual-hat" appointment underpins the close partnership between USCYBERCOM and NSA/CSS—a

significant benefit in cyberspace operations. The institutional arrangement for providing that support, however, may evolve as USCYBERCOM grows to full proficiency in the future, as I shall explain below.

The Cyber Threat Environment

The pace of international conflict and cyberspace threats has intensified over the past few years. We face a growing variety of advanced threats from actors who are operating with ever more sophistication and precision. At USCYBERCOM we track state and non-state adversaries as they continue to expand their capabilities to advance their interests in and through cyberspace and try to undermine the United States' national interests and those of our allies.

America faces multiple challenges from non-state cyberspace actors who impact our citizens and our economy, which now depends on trusted data. For instance, over the last year we have seen increased use of ransomware against individuals and businesses who find their data locked and are forced to pay in order to regain control of their files and intellectual property. Such threats primarily fall under the jurisdiction of law enforcement authorities, particularly the Federal Bureau of Investigation and the Secret Service. Nevertheless, criminal actors become a military concern when malicious state cyber actors pose as cyber criminals, or when cyber criminals support state efforts in cyberspace. This means that we take notice when cybercriminals employ tactics, techniques and procedures used by state adversaries.

My main concern relates to state-based cyber actors, whose malicious activities have only intensified since I spoke to this Committee last year. As we have seen, cyber-enabled destructive and disruptive attacks now have the potential to affect the property, rights, and daily lives of Americans. We are particularly concerned as adversaries probe and even exploit systems used by government, law enforcement, military, intelligence, and critical infrastructure in the United States and abroad. We have seen states seeking to shape the policies and attitudes of democratic peoples, and we are convinced such behavior will continue for as long as autocratic regimes believe they have more to gain than to lose by challenging their opponents in cyberspace.

At the operational level of conflict, states are incorporating cyber effects to support their military operations. As early as 2008, for instance, the Russian incursion in Georgia was accompanied by a denial-of-service attack against Georgia's government Internet services as well as the defacement of content on official web pages. We are not yet seeing true, combined-arms operations between cyber units and "kinetic" missions, although we have spotted hints of this occurring in Syria and Ukraine as the Russians attempt to boost the capabilities and successes of their clients and proxies. In general, these and other conflicts feature cyber operations by all sides; Russian government sites, for example, have sporadically been attacked by sympathizers from Ukraine. Advanced states continue to demonstrate the ability to combine cyber effects, intelligence, and asymmetric warfare to maintain the initiative just short of war, challenging our ability to react and respond. Further, states clearly continue to leverage cyberspace to conduct significant, widespread, intelligence operations. Access to large volumes of data enable Insider threats; defending against these is a critical requirement of the current and future landscape.

U.S. Cyber Command has seen indications that several states are investing military resources in mining the networks of the Department of Defense and its contractors. On a daily basis, state cyber actors coordinate and execute exploits and scans of the DoD Information Networks (what we now call the DoDIN) as well as related governmental and private systems. These activities are often automated, and they can include well-crafted spear-phishing expeditions. We assess that the motivation behind these efforts is predominantly espionage, but the mere possibility that an adversary might establish a persistent presence in DoD networks is always a grave concern; such intrusions, when they occur, are quite disruptive and expensive to remediate.

A still-greater concern is the persistence of adversary attempts to penetrate critical infrastructure and the systems that control these services. We assess that several countries, including Iran, have conducted disruptions or remote intrusions into critical infrastructure systems in the United States. Last year, for example, the Justice Department announced indictments of seven Iranians for cyber disruptions of U.S. financial institutions. The Attorney General reported that 46 U.S. companies together suffered tens of millions of dollars in losses as a result of the attacks. In addition, in late 2015 a malware tool (Black Energy) identified in energy-sector systems worldwide was implicated in a malicious cyber attack against Ukrainian power systems. The Department of Homeland Security has been warning systems administrators at critical infrastructure sites in the United States and abroad about sophisticated cyber threats from malicious actors employing Black Energy. In December 2015, the cyber actors who had deployed Black Energy in Ukraine briefly cut off electricity to hundreds of thousands of Ukrainians, possibly in support of Moscow's aims in Crimea and Eastern Ukraine. Infiltrations in US critical infrastructure—when viewed in the light of incidents like these—can look like preparations for future attacks that could be intended to harm Americans, or at least to deter the United States and other countries from protecting and defending our vital interests.

Violent extremist organizations constitute another focus for USCYBERCOM. For over a decade, they have used the Internet to publicize their malicious actions to intimidate opponents and win sympathizers. As we know from the reporting and analysis of respected journalists and think tanks, groups like ISIS conduct sophisticated multi-media campaigns that spread its messages swiftly and globally. While ISIS uses the Internet to recruit followers and solicit contributions in the West, its media campaign also effects viewers closer to home in the Middle East, boosting morale among ISIS fighters, frightening opponents, and promoting the false narrative that the Arab future inevitably belongs to a radical Salafist brand of Sunni fundamentalism. This information campaign through cyberspace has directly and indirectly impacted Americans, inciting attacks on Americans and the citizens of our European allies, who have suffered even worse assaults than we have seen here. Legitimate Internet media outlets obviously have no interest in lending social spotlights to terrorists by hosting violence or propaganda material, and regularly remove these messages and advertisements when they spot them (or the content is brought to the companies' attention). Yet ISIS is resilient and persistent, and continues to spread its message. In addition, ISIS and other violent extremists communicate over encrypted channels to maintain command and control of their operatives and forces.

Examples like these foretell an uncertain future. Several trends could complicate it still further, like the growing "Internet of Things" providing millions of new Internet-connected devices for adversaries to exploit. Today, consumers who can hardly keep up with patching their laptops and updating their cellphone operating systems are wondering how to upgrade the firmware on their home security cameras or Wi-Fi extenders to keep their families and homes from being victimized by malicious cyber actors. Technological developments are outpacing laws and policies, and indeed will have long-term implications that we have only begun to grasp.

US Cyber Command in Operation

Hardly a day has gone by during my tenure at USCYBERCOM that we have not seen at least one significant cyber security event occurring somewhere in the world. This has consequences for our military and our nation at large. I want to reiterate what I told this Committee last year: every conflict around the world now has a cyber dimension. "Cyber war" is not some future concept or cinematic spectacle, it is real and here to stay. The fact that it is not killing people yet, or causing widespread destruction, should be no comfort to us as we survey the threat landscape. Conflict in the cyber domain is not simply a continuation of kinetic operations by digital means, nor is it some Science Fiction clash of robot armies. It is unfolding according to its own logic, which we are continuing to better understand. We are using this understanding to enhance the Department's situational awareness and manage risk. In light of this trend, I am convinced that we as a nation created our own military capability in cyberspace not a moment too early. Our government and military have gone from wondering whether we have a systemic computer security problem to recognizing that the problem can spread in seconds.

Let me explain how our Department of Defense cyberspace capability has progressed at USCYBERCOM over the last year. The Cyber Mission Force attained initial operational capability, with the last team reaching this milestone in October 2016. Our component commanders are moving out to ensure our people get training and certifications required to reach full operational capability for each CMF team. Achieving FOC, however, is not the ultimate goal. We must ensure the CMF also achieves and sustains a high level of readiness, just like any other military force.

My first mission priority as Commander of USCYBERCOM remains the defense of the DoD information network, which encompass millions of network devices, hundreds of thousands of users, well over ten thousand network enclaves, the data they carry, and the networked technology embedded in weapon systems and other operational platforms. Real-world defensive cyberspace operations have sharpened USCYBERCOM's ability to detect, confine, and eradicate threats from DoD networks and systems. At the same time, adversary cyberspace operations have grown more sophisticated and assertive, resulting in intrusions that have strained the abilities and capacity of DoD cyber forces. With broad authorities to operate within DoD networks, USCYBERCOM has been able to experiment with operational models and tradecraft, improving the effectiveness and efficiency of defensive missions. Our techniques are being adopted and refined across the force, making intrusion response more predictable and effective. USCYBERCOM has improved DoD network defenses through the implementation of new

authorities, innovative command and control structures, and operations informed by offensive planning and intelligence (particularly signals intelligence).

USCYBERCOM executes its DoDIN defense mission in part through Cyber Protection Teams (CPTs)—the defense-focused forces within the CMF. These teams have real-world experience dealing with sophisticated intruders in DoD systems. The CPTs conduct internal defensive measures to protect key DoD terrain in cyberspace, coordinating with local defenders in the cybersecurity service providers, including those aligned to USCYBERCOM under Global Force Management guidance. The CPTs work with system owners, administrators, and local network defenders to find vulnerabilities and hunt for intruders inside DoD networks. This approach embodies the Department's shift to an operational mindset. Should adversary activity be detected, CPTs track, confine, and expel malicious actors using time-tested doctrinal principles consistent with those employed in the other domains. CPTs share what they learn with other network defenders, offensive operations planners, and the Intelligence Community. USCYBERCOM's continual efforts to adapt to the shifting threat environment have resulted in considerable gains to DoDIN security and resiliency.

In addition, as the operational sponsor of the Joint Information Environment (JIE), USCYBERCOM is working with partners to improve the security of the DoDIN. These efforts include implementation of Joint Regional Security Stack (JRSS) enterprise cybersecurity capabilities, integration of IT systems management into the cyberspace operations framework, and development of technical and operational frameworks that will enable establishment of comprehensive cybersecurity practices within DoD and mission partners.

The Defense Information Systems Agency serves as DoD's "Internet service provider" and thus plays a vital role in securing and defending the DoDIN. Its director is dual-hatted as the commander of one of USCYBERCOM's operational components, Joint Force Headquarters (JFHQ)-DoDIN, which is tasked with directing and executing global DoDIN operations and defensive cyberspace operations. This component oversees the Command Cyber Readiness Inspection (CCRI) process in collaboration with local network administrators. CCRIs help JFHQ-DoDIN assess DoDIN systems for compliance with cybersecurity directives and USCYBERCOM orders; inspections thus support USCYBERCOM and DoD Chief Information Officer-led efforts to improve the Department's cybersecurity accountability.

USCYBERCOM works with the Services, NSA and the Defense Cyber Crime Center (DC3) to ensure the CPTs are optimally manned, trained, and equipped. This includes development and acquisition of new capabilities as technology advances; the building of realistic training environments; and resourcing and refining of new models for CPT deployment and operations. USCYBERCOM also seeks to enhance the Department's situational awareness of the status of the DoDIN and adversary activities, to extend protection from the network level down to weapons systems, and to develop capabilities and common approaches for linking cybersecurity risk (beyond compliance) to mission assurance in order to inform warfighting decisions and mitigation efforts.

USCYBERCOM's missions extend far beyond the defense of the DoDIN. In particular, the Command supports the geographical and functional combatant commands in their operations

and missions. This is the business of the USCYBERCOM's Cyber Combat Mission Force. The Cyber Combat Mission Force is the operational-level offensive forces of the CMF, comprising Combat Mission Teams (CMTs) and Combat Support Teams (CSTs), aligned to the Combatant Commands to support their execution of military operations. The CMTs and CSTs are manned, trained, and equipped by their parent services, which exercise oversight of the combat forces they generated through the Joint Force Headquarters (JFHQ) associated with each Service cyber component.

USCYBERCOM is working to synchronize cyber planning and operations across the entire joint force. Since gaining the Secretary of Defense's approval for this proposal in early 2016, USCYBERCOM has implemented a process to allocate limited CMF resources among the commands as "high-demand, low-density" military assets. Currently in implementation, this process will enable USCYBERCOM to balance national and operational-level priorities, enabling the Chairman of the Joint Chiefs of Staff to guide the former through the Command in a crisis while providing tailored capacity forward to support the combatant commands when a situation moves towards actual conflict. USCYBERCOM is also helping the combatant commands build cyber effects into their planning processes so that cyberspace missions are synchronized with operations in the other domains. Indeed, in some situations, USCYBERCOM is the supported command.

Achieving Full Operational Capability in the Cyber Mission Force is our goal, but we acknowledge that reaching that milestone is only a capability metric and not a measure of overall readiness. CMF readiness is a shared responsibility between USCYBERCOM and the Services, and over the last 15 years of conflict we have recognized the costs of continuous operations and seen those costs grow the most in "high-demand, low-density" units – like our CMF teams. We employ teams before they are FOC, which is comparable to employing fighter squadrons before they are fully manned or equipped. Achieving and sustaining readiness is going to require a comprehensive set of solutions, ranging from an agreed upon readiness model between USCYBERCOM and the Services, to ensuring the manpower depth necessary to accommodate professional development, technical proficiency, and career predictability. I am confident we will achieve Full Operational Capability by our 30 September 2018 deadline, but I acknowledge that the true challenge will be sustaining the readiness of the CMF and the remarkable men and women who serve within the teams. We have a duty to them, and we must ensure that they are well trained, prepared, and mission-ready.

USCYBERCOM is executing its missions to support operations against violent extremists, especially across the US Central Command's area of responsibility (and is helping US Special Operations Command's efforts as well). About a year ago, Secretary Carter facilitated this support by issuing an execute order that, among other things, helped USCYBERCOM by authorizing us to "task organize" for specific missions expected to last weeks, months, or longer. The result of this change was a new organization, Joint Task Force (JTF)-Ares, established by me as the Commander of USCYBERCOM in the spring of 2016 to coordinate cyberspace operations against ISIS. JTF-Ares' mission is to provide unity of command and effort for USCYBERCOM and coalition forces working to counter ISIS in cyberspace. The JTF model has helped USCYBERCOM to direct operations in support of

USCENTCOM operations, and marks an evolution in the command-and-control structure in response to urgent operational needs.

JTF-Ares has helped strengthen unity of efforts against ISIS across international coalition and domestic partners, reinforcing USCYERCOM's informal role as a hub for whole-of-government cyber planning and execution against terrorist organizations and targets. Cyber effects can be achieved at-scale and with remarkable synchronization when mission partners share plans, accesses, capabilities, and tactics in support of common objectives. USCYBERCOM, working with the National Counterterrorism Center (NCTC) and the various departments and agencies engaged in this campaign, is using opportunities such as the defeat-ISIS campaign to build trust among operational partners.

USCYBERCOM expects to make progress through 2018 in several key areas. The Command will complete the CMF build, work with DoD partners to equip the CMF, resource and refine command-and-control structures and processes, and develop policies, plans, and operational concepts that support national-level and joint warfighting needs. USCYBERCOM seeks with DoD and Intelligence Community partners to overcome organizational and technological challenges associated with supporting offensive operations at the strategic, operational, and tactical levels. Finally, USCYBERCOM will collaborate with allies and partners to enable collective defense and develop cyber "response actions" that provide options to decision makers from pre-crisis through kinetic operations across all phases of conflict.

Defending the nation in cyberspace is complex in both technical and policy terms. Like all Combatant Commands, USCYBERCOM is authorized only on order from the President (or the Secretary of Defense if the President is unavailable) to defend against a threat to the nation that would qualify as a "use of force" under international law. The Cyber National Mission Force (CNMF) focuses on countering adversaries' malicious cyber activities against the United States and prepares to conduct full-spectrum cyber operations against adversaries when directed. The CNMF is building a force of National Mission Teams (NMTs), National Support Teams (NSTs), and National Cyber Protection Teams (N-CPTs). Partnering with NSA, the CNMF tracks adversary cyber actors to gain advantages that will enable the United States to preclude cyber-attacks against US national interests. The CNMF is working with operational partners to develop and exercise the capabilities and operational concepts needed to enable combined and coalition operations (when authorized) in partnership with other government and appropriate private-sector partners.

USCYBERCOM manages only a portion of the "whole-of-nation" effort required to defend America's critical infrastructure. The Command works with civilian agencies under their authorities to help protect national critical infrastructure and to prepare for scenarios in which US military action to defend the nation may be required.[1] The Command is expanding its ties with the Reserves and the National Guard. Indeed, cyber response teams operating under Guard authorities can perform a variety of missions in support of state, local, and private entities (which operate independently under their own authorities). Recent legislation to incentivize information

[1] The Department of Justice (particularly the Federal Bureau of Investigation) is the lead for cyber-related investigations and law enforcement, while the Department of Homeland Security takes the lead for national protection and recovery from cyber incidents.

sharing will also help the Command and DoD to work more closely with the private sector in mitigating threats outside of government and military systems. The federal government has created a framework for implementing official channels to share information, and clarifying the lanes in the road for US government assistance to the private sector. Whatever USCYBERCOM's ultimate role in that process is determined to be, I continue to tell all audiences that we adhere strictly to the Constitution and law in guarding civil liberties and privacy.

The Command is increasing its efforts in the areas above in alignment with the 2015 *DoD Cyber Strategy*. The Department, as you know, is engaged in a broad effort to improve the security of its information enterprise and to build a culture of cybersecurity. Doing so requires measures well beyond hardening the network architecture, and it cannot be accomplished in just a year or two, even with unlimited resources. The strategy is to replace the old infrastructure, to harden what we are maintaining while increasing its capability, and to grow a workforce possessing outstanding cybersecurity awareness and practices. Beyond that, we must understand that determined adversaries can sometimes bypass even the best security, and thus we must build our skills, as well as an operational mindset, for defeating them in our own networks.

These efforts, of course, depend on skilled, focused, and motivated people in a trained and ready force. USCYBERCOM tapped the expertise of NSA to deliver intensive training for cyber personnel, initially taking the lead in training operators from the Service cyber components who graduate to join the CMF teams. This hybrid arrangement will come to an end, with the Services resuming responsibility and authority for training CMF personnel at the end of 2018. In keeping with DoD's Total Force concept, the Reserve component and the National Guard will also help to build the force. This requires flexibility with organizational requirements and manning standards, but it is already helping to increase the manpower and expertise we can put against some of our most difficult challenges.

USCYBERCOM is maturing its methods for identifying requirements and developing capabilities. The Command last year established a capabilities development team for performing this task, and that group has already done much good. It is doing so not only by working with industry, academia, and other agencies to identify promising ideas, but also in learning how to utilize the data we already generate from our own operations (particularly on DoD systems) to spot useful and/or anomalous patterns. The Command generally lacks NSA's authorities in acquiring the tools for such initiatives, but Congress recently authorized USCYBERCOM acquisition authority for up to $75 million each year through the end of FY2021 to rapidly deliver acquisition solutions for "cyber operations-peculiar" capabilities. We look forward to reporting to the Committee soon on how we are executing this authority.

USCYERCOM has now matured to the point where it brings vital capabilities to the defense of American interests on a daily basis. In light of the increasing severity of cyber threats, Congress in the National Defense Authorization Act for FY2017 directed the President to elevate USCYBERCOM to the status of a full unified combatant command. Elevation implicitly recognizes the importance of cyberspace to our national security. I support this step, although the timing and process for elevation are being worked out within the Department, and we expect to have more details to report to the Committee as they emerge. We will pay particular attention

to the implementation of the Act's provisions regarding authority for the acquisition of "cyber operations-peculiar" capabilities. As you know, the language in this section parallels that granted to US Special Operations Command. USSOCOM's requirements, however, are not always congruent with those to support operations in the cyberspace domain, and thus authorities in the one field might not always be directly analogous to those in other. We are working with Committee staff to ensure that our implementation comports with Congress's intent.

The recent National Defense Authorization Act in a separate provision also described some conditions for splitting the "dual-hat" arrangement, once that can happen without impairing either organization's effectiveness. This is another provision I have publicly stated I support pending the attainment of certain crucial conditions. I have offered this caveat because the challenges in cyberspace are some of the greatest facing America. Meeting tomorrow's threats requires leaders who can devote their time and energy to building the capabilities of USCYBERCOM and NSA while guarding the rights and liberties of US persons protected by our Constitution. We have not yet matured the Command to a point where splitting the two hats would not functionally impair mission effectiveness. If that point is reached on my watch, I intend to keep the Committee fully informed of the conditions set for the split and how they are met.

USCYBERCOM will also engage with this Committee on several other matters relating to the enhancement of the Command's responsibilities and authorities over the coming year. These would include enhancing the professionalization of the cyber workforce, building capacity and developing capabilities, and streamlining acquisition processes. Most or all of these particulars have been directed in recent National Defense Authorization Acts; and along with the Office of the Secretary of Defense for Policy and the Joint Staff, we will be talking with you and your staffs to iron out the implementation details.

Conclusion

Thank you for inviting me to talk with you today about US Cyber Command and its work. The Cyber Mission Force approaching full operational capability, and USCYBERCOM is poised to become a mature unified combatant command. USCYBERCOM personnel are proud of the roles they play in this endeavor, and are motivated to accomplish the many missions assigned to them and overseen by the Congress, particularly this Committee. They work to counter adversaries and support national and joint warfighter objectives in and through cyberspace on a previously unattainable scale and in a sustainable manner. Innovations are constantly emerging out of operational necessity. These, if supported with agile policies, decision-making processes, capabilities, concepts of operation, and command and control structures, will help USCYBERCOM realize its potential to counter adversary cyber strategies in and through cyberspace. The Command's full-spectrum successes have validated concepts for creating cyber effects on the battlefield and beyond. Real-world experiences in meeting the requirements of national decision-makers and joint force commanders have driven operational advances that need time to mature. With the Cyber Mission Force now at initial operational capability, USCYBERCOM is demonstrating its contribution to comprehensive US Government approaches to countering adversary strategies in and through cyberspace.

The men and women of US Cyber Command thank you for your support, both in the past and in the big tasks ahead of us. We understand that a frank and comprehensive engagement with Congress not only facilitates the support that allows us to accomplish their missions, but also helps ensure that our fellow citizens understand and endorse our efforts on their behalf. I have seen the growth in the command's size, budget, and mission. That investment of resources, time, and effort is paying off, and more importantly, is helping to keep Americans safer, not only in cyberspace but in the other domains as well. I look forward to continuing the dialogue over the Command and its progress with you in this hearing today and over the months to come. And now I would be happy to address your specific questions and concerns.