[H.A.S.C. No. 115–47]

HEARING

ON

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2018

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES HEARING

ON

FISCAL YEAR 2018 BUDGET REQUEST FOR U.S. CYBER COMMAND: CYBER MISSION FORCE SUPPORT TO DEPARTMENT OF DEFENSE OPERATIONS

HEARING HELD
MAY 23, 2017

U.S. GOVERNMENT PUBLISHING OFFICE
25–869 WASHINGTON : 2018

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

ELISE M. STEFANIK, New York, *Chairwoman*

BILL SHUSTER, Pennsylvania
BRAD R. WENSTRUP, Ohio
RALPH LEE ABRAHAM, Louisiana
LIZ CHENEY, Wyoming, *Vice Chair*
JOE WILSON, South Carolina
FRANK A. LoBIONDO, New Jersey
TRENT FRANKS, Arizona
DOUG LAMBORN, Colorado
AUSTIN SCOTT, Georgia

JAMES R. LANGEVIN, Rhode Island
RICK LARSEN, Washington
JIM COOPER, Tennessee
JACKIE SPEIER, California
MARC A. VEASEY, Texas
TULSI GABBARD, Hawaii
BETO O'ROURKE, Texas
STEPHANIE N. MURPHY, Florida

KEVIN GATES, *Professional Staff Member*
LINDSAY KAVANAUGH, *Professional Staff Member*
NEVE SCHADLER, *Clerk*

CONTENTS

FISCAL YEAR 2018 BUDGET REQUEST FOR U.S. CYBER COMMAND: CYBER MISSION FORCE SUPPORT TO DEPARTMENT OF DEFENSE OPERATIONS

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES,
Washington, DC, Tuesday, May 23, 2017.

The subcommittee met, pursuant to call, at 3:37 p.m., in room 2118, Rayburn House Office Building, Hon. Elise M. Stefanik (chairwoman of the subcommittee) presiding.

OPENING STATEMENT OF HON. ELISE M. STEFANIK, A REPRESENTATIVE FROM NEW YORK, CHAIRWOMAN, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Ms. STEFANIK. The subcommittee will come to order. I want to welcome everyone to today's hearing of the Emerging Threats and Capabilities Subcommittee of the House Armed Services Committee [HASC].

With the President's budget request released just earlier today, this is our first opportunity to explore this request and the major implications for key defense missions. I think it is fitting that the first area we will dive into is cyber. This is an increasingly important domain of warfare and an area where we have increased our emphasis on overseeing the Department's progress in building and maintaining cyber forces to protect, defend, maintain, and, when necessary, conduct offensive operations in cyberspace.

As we move towards developing the fiscal year [FY] 2018 NDAA [National Defense Authorization Act], I have made cyber and cyber warfare one of my main priorities. In the coming weeks, Chairman Mac Thornberry and I, in addition to my ranking member, Jim Langevin, and the HASC ranking member, Adam Smith, plan to introduce standalone cyber warfare legislation that strengthens congressional oversight of sensitive military cyber operations, including mandating prompt notifications to Congress in the event of unauthorized disclosures.

We look forward to continuing to work with U.S. Cyber Command [CYBERCOM] and the Department of Defense [DOD] as we finalize this draft legislation to ensure such notifications are responsive to our needs but without adding undue reporting burdens on the Department of Defense.

In addition to our focus on strengthening congressional oversight in the area of cyber warfare, other key focus areas will include provisions to strengthen our own cyber warfare capabilities and provisions that enhance our international partnerships across the globe.

In order to more thoroughly understand all of these issues, I would like to welcome our witness today, Admiral Mike Rogers, who serves as the Commander of U.S. Cyber Command and the Director of the National Security Agency [NSA].

Let me now recognize Ranking Member Jim Langevin for any opening comments he would like to make.

[The prepared statement of Ms. Stefanik can be found in the Appendix on page 29.]

STATEMENT OF HON. JAMES R. LANGEVIN, A REPRESENTATIVE FROM RHODE ISLAND, RANKING MEMBER, SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Mr. LANGEVIN. Thank you, Madam Chair.

And welcome, Admiral Rogers. I want to thank you for testifying before us today. It is always a pleasure to have you before the subcommittee. And thanks for bringing along a crowd. It makes it a little more of an interesting hearing.

So the President's budget for fiscal year 2018 was delivered just this morning, as the chair stated, and so I look forward to hearing about priority investments in cyber and about any potential new legislative initiatives relating to cyber.

Last year, Congress passed legislation establishing U.S. Cyber Command as its own unified combatant command. This subcommittee worked diligently on the underlying legislation because we recognized the importance of a trained and ready force able to conduct effective cyber operations in concert with other military and U.S. Government efforts, consistent with the appropriate legal authorities and policies.

The FY 2017 NDAA also formalized the relationship with the Principal Cyber Advisor to ensure advocacy and oversight of the command. We also provided U.S. Cyber Command with limited cyber-peculiar acquisition authorities 2 years ago, and I would like to acknowledge the thoughtfulness by which the Department has implemented this authority.

Today I look forward to hearing about where these two initiatives stand, both the process by which necessary resources are being transferred from STRATCOM [Strategic Command] to CYBERCOM and the new resources being provided as necessary for effective implementation.

Clearly, we have made progress employing military cyber operations over the years. We have been building the Cyber Mission Force, but now we must make sure that they are ready and stay ready for a threat that morphs on a daily basis. The persistent training environment, of course, is key to that end.

Although the cyber domain is not new, there is still much that we are learning, and we must leverage those lessons learned. We must assess the force we are building, how we employ it, in order to ensure CYBERCOM is postured correctly and that the tools and capabilities are the best that we can provide them.

So next week, I am going to be traveling to NATO [North Atlantic Treaty Organization], the NATO Cooperative Cyber Defence Centre of Excellence, to attend its annual conference in Tallinn, Estonia. I expect that CyCon [Conference on Cyber Conflict] will provide extraordinary insight on how our NATO allies view the cyber

domain and how international laws are applicable. And it will provide me with insight on how we can increase cyber collaboration against Russian aggression.

Admiral, I would also appreciate your views on how we may strengthen collaboration with our NATO allies.

So in closing, I just want to echo what the chair said about the importance of formalizing notifications to Congress of sensitive cyber military operations. The cyber quarterly brief provides us a forum to oversee cyber operations, and I was especially pleased with the participation of the Joint Staff and OSD [Office of the Secretary of Defense] at the last engagement. However, in our oversight capacity, I believe that we must work with the Department to obtain timelier, more standard notifications, as the chair mentioned, and I know that we are going to work toward that end.

So with that, I thank you, Admiral Rogers, for appearing today. Thank you for what you are doing at NSA and U.S. Cyber Command.

And with that, I will yield back.

Ms. STEFANIK. Thank you, Jim.

I also would like to remind members that immediately following this open hearing the committee will reconvene upstairs in 2337 for a closed classified roundtable discussion with our witness.

Admiral Rogers, you are now recognized for your opening statement.

STATEMENT OF ADM MICHAEL S. ROGERS, USN, COMMANDER, U.S. CYBER COMMAND

Admiral ROGERS. Thank you. Chairwoman Stefanik, Ranking Member Langevin, and members of the subcommittee, thank you for your enduring support and the opportunity today to talk about the hardworking men and women of the United States Cyber Command.

I look forward to discussing the command's posture, and I welcome the opportunity to describe how U.S. 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 us 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 past 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 operate with ever more sophistication 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 continue to better understand. And we are using this understanding to enhance the Department's and the Nation's situational awareness and to manage risk in the cyber arena.

I would also look forward to updating you on our initiatives and plans to help do that. Our three lines of operation 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 U.S. and allied freedom of action in cyberspace, and deny the same to our adversaries. Defense of DOD information networks remains our top priority, of course, and that includes weapon systems and their platforms as well as data.

To execute our missions, I requested a budget of approximately $647 million for fiscal year 2018, which is nearly a 16 percent increase from fiscal year 2017 due to additional funding for Cyber Command's elevation per the fiscal year 2017 NDAA, building out Cyber Mission Force and cyber-specific capabilities and tools and JTF-Ares [Joint Task Force-Ares] support in the fight against ISIS [Islamic State of Iraq and Syria].

We are completing the buildout of the Cyber Mission Force with all teams scheduled to be fully operational by the end of fiscal year 2018, and with the help from the services, continually increase Cyber Mission Force readiness to hold targets at risk. Your strong and continued support is critical to the success of the Department in defending our national security interests in cyber.

As you well know, I serve as both Commander of United States 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 right now in cyberspace operations. The institutional arrangement between these two organizations, however, will evolve as Cyber Command grows to full proficiency in the near future.

The National Defense Authorization Act in a separate provision also described conditions for splitting the dual-hat arrangement, which can only happen without impairing either organization's effectiveness and ability to execute their missions. This is another provision I publicly stated I support pending the attainment of certain critical conditions.

Cyber Command will also engage with this subcommittee on several other matters related to the enhancement of the command's responsibilities and authorities in the coming year. This would include increasing cyber manpower, enhancing the professionalization of the cyber workforce, building defensive and offensive capability and capacity, and developing and streamlining our acquisition processes.

These are critical enablers for cyberspace operations in a dynamically changing global environment. And most or all of these particulars have been directed in recent NDAA acts. Along with the Office of the Secretary of Defense for Policy and the Joint Staff, we will talk with you and your staffs to iron out the implementation details of that legislation.

The men and women of Cyber Command are proud of the roles that we play in our Nation's cyber efforts and are motivated to accomplish our assigned missions overseen by the Congress, particularly this subcommittee. We work to secure and defend DOD systems and networks, counter adversaries, and support national and joint warfighting 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 in meeting the requirements of national decision makers and joint force commanders continue to mature our operational approaches and effectiveness over time.

At the same time, I realize cybersecurity is a national security issue. It requires a whole-of-nation approach that brings together both public and private sections of our society.

Our Point of Partnership program in Silicon Valley and Boston has proven to be a successful initiative to link our command to some of the most innovative minds from industry, working together on cybersecurity as we face 21st century threats together in the private and public sectors.

This, combined with agile policies, decision-making processes, capabilities, and command-and-control structures, will ensure that Cyber Command attains its potential to counter our adversaries.

The men and women of U.S. Cyber Command thank you and appreciate your continued support as we confront and overcome the challenges facing us. We understand that a frank and comprehensive engagement with Congress not only facilitates the support that allows us to accomplish our mission but also helps ensure that our fellow citizens understand and endorse our efforts, which are executed on their behalf.

I have seen the growth in our command's size, budget, and mission, and that investment of resources, time, and effort is paying off; and more importantly, it is helping to keep Americans safer in the cyber arena, not only in cyberspace but in other domains as well. And I look forward to continuing the dialogue across the command and its progress with you in this hearing today and over the months to come.

I look forward to answering your questions.

[The prepared statement of Admiral Rogers can be found in the Appendix on page 30.]

Ms. STEFANIK. Thank you, Admiral Rogers.

We now turn to questions. First, I want to thank you for your service and your leadership.

My first question is very broad. Last year's NDAA directed the elevation of Cyber Command to a full combatant command. What steps need to happen before the changes to the Unified Command Plan take effect?

Admiral ROGERS. So, first, the Secretary of Defense and the President need to make a decision, the Secretary of Defense making a recommendation, the President ultimately making the decision as to the timing and the process we will use. And that process is ongoing, and I don't want to speak for the Secretary or the President, but I know that that process and that discussion is ongoing.

Given the language in the NDAA and in anticipation of this possibility, we have spent much of the last year working our way through the specifics of how we would do that. And if a decision is ultimately approved, we are prepared to apply that and to do it in a timely manner in accordance with the direction in terms of the timeline provided to us via the President and the Secretary of Defense.

Ms. STEFANIK. What are the specifics? As you said, you are assessing the specifics you would do to take action. What are they specifically?

Admiral ROGERS. So if I could, until we have an ultimate decision, I would rather not get ahead of my leadership, because I think I owe them that, and to get into the how, if that would be all right, ma'am.

Ms. STEFANIK. Yes.

Part of your responsibilities that we enshrined in section 923 of FY 2017 NDAA when we elevated CYBERCOM to the full combatant command involved development of doctrine and tactics related to cyber. What role do you have in advocating for or driving doctrinal development for the individual services when it comes to cyber?

Admiral ROGERS. So as the senior operational commander in cyber in the Department, it is the partnership between that cyber team, if you will, and our fellow operational commanders and policy makers that help shape: So what is the doctrine that should shape how we employ this capability that the Department is developing?

If you look at what we have done over the course of the last year, the efforts against ISIS, things we are doing against other real world challenges, they are shaping the way we are looking at how do we build the force of the future, what are the concepts for its employment.

If you go back a couple years, for example, I can remember a year ago, 2 years ago, one of our fundamental concepts was we are always going to deploy forward and full teams. One of the things we found with practical experience is we can actually deploy in smaller sub-elements, use reach-back capability, the power of data analytics.

We don't necessarily have to deploy everyone. We can actually work in a much more tailored, focused way, optimized for the particular network challenge that we are working. We are actually working through some things using this, for example, out in the Pacific at the moment.

Ms. STEFANIK. A few weeks ago in your testimony in front of SASC [Senate Armed Services Committee], you were asked your opinion about whether we should be considering the establishment of a cyber service, and at that time you said that you were not a proponent. Could you explain a bit more as to why you feel that way?

Admiral ROGERS. Yes, ma'am.

So the reason I am not a—I certainly understand others have a different view—the reason I am not a proponent of that is, my concern is, if we are not careful, we will view cyber as this very technical, very specialized, very narrow mission set. And my view is cyber fits within a broader context. And if you want to be successful in the ability to achieve outcomes within the cyberspace arena, you need to understand that broader context.

And I am afraid that if we go the service route, we will tend to generate incredibly technically proficient but very narrowly focused operators. And one of my takeaways from being a member of the Department of Defense for the last 36 years is we are best optimized for outcomes when our workforce has a much broader perspective.

And I also think back—because I am a big fan of history—I think back to the dialogue in the 1980s when I first joined, was first commissioned in the military. In the aftermath of the failure of Desert One and the effort to rescue those U.S. hostages being held in the embassy in Tehran, we had a lot of dialogue about is SOF [special operations forces] so specialized, so poorly understood by the broad conventional part of the military, so needing of specific attention that we should create a separate SOF service.

We ultimately decided that the right answer was to create a joint warfighting construct. Thus, in 1987 was born Special Operations Command [SOCOM]. And in addition, we said that that operational entity needed to be a little uniquely structured. It not only should be a warfighter, but it should be given budget resources that enable it to not only employ capability but to determine the operational capabilities that actually, and drive the investments that actually generate the capability.

I think that that is a very effective model for us to think about for cyber and Cyber Command vice just automatically transitioning to the idea of a separate service.

Ms. STEFANIK. Thank you. My time is about to expire.

I now recognize Mr. Langevin.

Mr. LANGEVIN. Thank you, Elise.

So, Admiral, Congress has provided CYBERCOM with limited cyber-peculiar acquisition authority. So I want to first of all commend the thoughtfulness by which the provision was implemented. But can you please provide a general overview of how that authority will be executed and overseen in the command.

Admiral ROGERS. So as you are aware, we sat down between OSD from a policy and technical perspective and Cyber Command from an operational perspective and asked ourselves: What is the best way to implement this acquisition authority that was granted to us by the Congress?

Again, we thought SOCOM offered a good model. We actually—Cyber Command actually approached our teammates in SOCOM and said: Look, you have a skill set, you have personnel who are much more proficient in this area than we.

So SOCOM was kind enough to actually identify the two initial individuals that we have hired who are going to provide our acquisition, oversight, and certification, if you will. Those individuals

were put in place just a couple months ago. The authorities are now almost all finished.

What you are going to see starting this summer is we have identified an initial set of priorities about where we want to apply this authority in terms of acquisition, and you will see that play out over the course of the next couple of months. We have just got a couple of things we have to finish ironing out. But you are going to see us actually implement this over the course of the next few months in the summer.

Mr. LANGEVIN. So it has not, the authority has not been used yet?

Admiral ROGERS. Not yet. There are some specific technical and oversight and control things I have to make sure are in place before we start spending the money and using this. That will all be finished within the next month or so, I think.

Mr. LANGEVIN. Can you speculate, just provide an example of what you think the authorities may be used for.

Admiral ROGERS. So what I have asked is we have already identified, for example, a series of capabilities through Cyber Command's Point of Partnership, we call it, out in Silicon Valley. So I already have a structure that is interacting with the private sector.

Now I want to overlay this acquisition authority to actually now—I actually purchase, if you will, and acquire some of that capability from the private sector that we have been talking to them about now for the last few months.

So I try to work the requirement piece in anticipation of gaining the acquisition authority. Now that we have got that pretty much done and I overlay the acquisition authority, you are going to see us start to enter into some specific contracts very focused on a couple of specific mission sets. Defense capability for cyber protection teams is the first area we are going to focus on.

Mr. LANGEVIN. Okay. Very good.

So I mentioned in my opening statement that I am going to be attending the annual cyber conference at NATO, the Cooperative Cyber Defence Centre of Excellence next week. What is Cyber Command's relationship with the center and NATO? And in your opinion, how can we cooperate more closely with our NATO allies? How can that cooperation be strengthened?

Admiral ROGERS. So, for example, like yourself, I was just out there last June, spoke at the same conference you will be going to next month. Every time I am in Estonia I spend time at the center and actually talk to them. The points I try to make to my NATO teammates are a couple-fold.

First, under the NATO framework, the center represents the positions of the members of the alliance that participate in the center, not necessarily the alliance as a whole. So for example, not all 28 nations—29 now with Montenegro—not all 29 nations actually participate in the center. I would like to see if we can somehow more formally tie the center to NATO's policy development, for example. I think that could really accelerate some things.

Also, I am trying, because capacity is certainly a challenge, and I am trying to both meet our own priorities as well as help key allies in the NATO alliance. One of the things I am interested in is I have created a partnership with European Command. We are

talking about potentially placing an individual maybe in the center in the course of the next year or so to more directly link with ourselves.

I would also like to see what could we potentially do within the exercise framework that the alliance is starting to create in cyber now. I have already extended invitations to them to observe and participate in our exercise framework, but I would like to do the same thing, if I could, within the NATO arena.

Mr. LANGEVIN. So you know that, obviously, the Congress passed the CISA, the cyber information-sharing legislation, and that is something, obviously, domestically.

Admiral ROGERS. Right.

Mr. LANGEVIN. But also we have robust cyber threat information sharing, for example, with the Israelis.

How are we doing with robust cyber threat sharing information with our NATO partners?

Admiral ROGERS. Right now, most cyber sharing tends to be focused in many ways on a nation-to-nation basis. That is another one of the challenges that I am interested in with Cyber Command, how can we work that more formally or military organization to military organization so we are doing this once and not 29 different times, as it were.

Mr. LANGEVIN. Okay. Very good.

Well, my time has expired. I do have additional questions, but if we don't get to a second round, I will submit them for the record. I appreciate your getting back to me on them.

But thank you, Admiral, for the work you are doing, and thanks for your service to the country. I yield back.

Ms. STEFANIK. Dr. Abraham.

Dr. ABRAHAM. Thank you, Madam Chair. Thank you, Admiral, for being here. I appreciate it.

Admiral ROGERS. Thank you.

Dr. ABRAHAM. The other services in the armed services certainly have their own cyber commands. What is CYBERCOM doing as far as the manning and the concept of operations as far as having duplicative issues within those services——

Admiral ROGERS. So, remember, the way——

Dr. ABRAHAM [continuing]. To prevent the duplication?

Admiral ROGERS. So the way we are structured, each of those service primary operational cyber commands is a subcomponent of U.S. Cyber Command. So whether it is Army Cyber, Coast Guard Cyber, Air Force Cyber, Fleet Cyber, MARFORCYBER [Marine Forces Cyber], they have an operational relationship to me. And so that is how we try to work the joint and the service piece in a very integrated way.

I am the first to acknowledge—and I was a service component commander before this job. I was the Navy's guy. I was Fleet Cyber Command. In those service structures, they are both OPCON [operational control] to me in the execution of their joint responsibilities, but they also have additional service responsibilities. And I try to be the connecting loop partnering with them and also partnering with the service leadership to make sure that from a service and a joint perspective within the Department we are aligned and focused on priorities and outcomes.

Dr. ABRAHAM. All right. And so let's parlay that into our other Federal agencies. It seems all of them certainly have a cyberspace department, so to speak. CYBERCOM, as far as coordinating mechanisms between other Federal agencies, could you explain that a little bit, please?

Admiral ROGERS. So we coordinate directly, primarily, in the rest of the government with the Department of Homeland Security [DHS]. That is particularly driven by the fact that one of Cyber Command's three missions is, if directed by the President or the Secretary of Defense to defend critical infrastructure against acts of significant cyber consequence, we would do that in partnership with DHS.

And so because of that, we are closely aligned with them. And, in fact, I just was talking with the team yesterday. Between the private sector—in the private sector the U.S. Government has designated 16 different areas. Think about finance, transportation, aviation. There are 16 different segments that the Federal Government has designated as critical to the Nation's security, that infrastructure.

We have picked one of those 16 segments to do a test case, if you will, between DHS, Cyber Command, that private sector, as well as NSA, from an information and intelligence sharing—that would be the NSA role—to try to get down to execution-level detail about so how would we really do this day-to-day. Because my experience as a military individual has taught me, I don't like to do discovery learning when I am moving to contact against an opponent. It tends to be high loss rate, incredibly inefficient and ineffective, often very resource intensive, and much slower.

So I am interested, how can I create those relationships and exercise them now before we get into a major incident directed against one of those 16 segments.

Dr. ABRAHAM. Okay. I think I have time for one more question.

What is CYBERCOM's supporting role in NORTHCOM [Northern Command], PACOM [Pacific Command]? And has the DOD codified that relationship so that if there is an incident or accident, that that could be really instituted very seamlessly if such an event should happen?

Admiral ROGERS. So our role on the defensive side is to support and ensure the continued operation, for example, of those networks, weapon systems, and platforms that those operational commanders and others count on to execute their missions.

In addition, we generate offensive capability, particularly for PACOM and other geographic commands outside the United States, because we don't really see, I don't think, right now in my mind, how would we apply cyber offensive capability in the United States. That is not the role of the DOD. Our focus inside the United States would be largely defensive.

One of the things that is a focus area, I have set out a series of goals for 2017. One of those goals is increased cyber Reserve and Guard integration, to get to the question that you are really driving at: How do we make sure that for a domestic incident that all elements of DOD are aligned, and we all know how we are going to do this, and all the forces know what their role is going to be, the command and control is all outlined, so NORTHCOM knows what

they are going to do, I know what I am going to do, PACOM, because they have a portion of a domestic responsibility, so that they know what they are going to do?

I would like to use the defense support to civil affairs, which has been an ongoing process we have used for decades, I would kind of like to use that as a test model. I am a big fan of let's use what is working elsewhere, let's not try to create something different or unique for cyber to the maximum extent that I can.

Dr. ABRAHAM. Okay. Thank you.

Ms. STEFANIK. Mr. Larsen.

Mr. LARSEN. Thanks, Admiral, for coming.

I would like to go back to the question of a unified Cyber Command, because your answer—I wasn't concerned about the answer—the portion of the answer, like we are still working it out. I was concerned because I thought I heard you say something that runs counter to what we told you all to do, and that is the decision is made to do this, and that the Secretary and the President don't need to make a decision to actually do a unified command. The law, as I understand——

Admiral ROGERS. But the time—they will drive the——

Mr. LARSEN. The timing of that, that is something separate.

Admiral ROGERS. Right. So that is my only point, is the timing piece.

Mr. LARSEN. If that is your only point, that is fine. I thought I heard something else.

Admiral ROGERS. No. I apologize if I miscommunicated. You have clearly provided a legal framework. It is what you are doing. You know, absent a change in the law, that is what we have to execute.

Mr. LARSEN. Okay. I appreciate that.

And I would like to go back as well to something the chair was exploring with you, and it has to do with having a cyber service or not. I actually agree with you in not having one. But it does beg the question, though: To have that capability, what flexibility do you need in personnel? What flexibility do you need in contracting? Just kind of what flexibility do you need to fully utilize and even develop a formal framework so you are using Active Component, Reserve, Guard, as well as the contractor community?

Admiral ROGERS. So among the ways that we try to ask ourselves: So if we are going to go with a service-based approach, which is really what we are executing, how would you do it? We came up with a couple of baseline principles, if you will.

The first is, it doesn't matter what your service is and it doesn't matter if you are Guard or Reserve. We build to one standard. And so we have created within a joint framework for every position within the Cyber Mission Force we can tell you what the pay grade is, and we can tell you what the qualification standards are, and we can tell you what the duties are that are assigned to the position. Because I said, look, we have got to create one integrated force, and if we do 1,000 different variants, I can't optimize that.

The second thing we said was the structure of the teams needs to be the same regardless of whether it is a particular service, Guard, or Reserve. The analogy I used was, it doesn't matter if we have an F–16 squadron in the Guard or in the Active force, there is one squadron nomenclature for an F–16 that we can then employ

anywhere globally, because we know everybody is built to the same standard. Even as we acknowledge there are some variances, but everybody is built to the same standard.

So that was another principle. I said, the only way we can make a service-based approach work is that Active or Reserve, Guard or Reserve, it doesn't matter. We are building to one standard.

If we stick to that framework, I am very comfortable that we can make a service approach work for us. If we insist on variance, if we insist on everybody doing their own thing, I am the first to admit, boy, this is not a model that is going to generate the outcomes that we need. I am the first to acknowledge that.

Mr. LARSEN. And the role of the private sector?

Admiral ROGERS. So the private sector, when I look at them, a couple things come to mind. Number one, they are providing, they are the ones who are going to provide the human capital, whether that human capital ends up wearing a uniform, whether it is part of our civilian government workforce, or it is contractor force, they all start in the private sector.

So it is one of the reasons why I spend a fair amount of time at Cyber Command and as the Director of NSA for that to the same extent in some ways, with the academic world, with private industry, about: So tell me how you create a workforce. What works for you? What incentives are you using? What has failed that in hindsight you say to yourself, "Boy, don't go down this road because it really failed spectacularly for us"? Even as I acknowledge there is a difference between government and the private sector, but I still think there are some things that we can learn from each other.

In addition, I think two other areas come to mind for me with the private sector. The first is technology. The days when DOD is going to be the engine for technological innovation and change I think are long behind us. That is just not the DOD model. That is why we created the Point of Partnership in Silicon Valley and in Boston. It is why I thought the acquisition piece was so important for us. We have got to be able to tap into that private sector in terms of acquisition of technology and capability.

And then the last area, which is a little bit counterintuitive in some ways, when it comes to the generation of policy, concepts, thought, the private sector can play a huge role here.

I think back to the beginnings of nuclear deterrence and nuclear policy, for example. If you go back in the 1950s and you read much of the thought process, much of that was flowing from the academic world. Hardly anybody remembers now that Henry Kissinger in the 1950s and early 1960s was a professor at Harvard who was writing about concepts of nuclear deterrence, nuclear employment that ended up, he and others, ended up shaping the strategic vision we had. And I would like to see us do the same thing in cyber.

Mr. LARSEN. Thank you.

Ms. STEFANIK. Ms. Cheney.

Ms. CHENEY. Thank you, Madam Chairwoman. And thank you, Admiral Rogers, for your service and for being here today.

Secretary Mattis, before he became Secretary, in talking about the Budget Control Act [BCA] and sequestration, said no foe in the field could do our military as much harm as has been done to us through sequestration and the Budget Control Act.

As we begin the process of looking at the 2018 budget, I am interested to know to what extent you were able to factor in strategy and threats and sort of strategic thinking about what needs to be done as you put together the budget for Cyber Command and to what extent you have still been hamstrung by the BCA and by those cap numbers.

Admiral ROGERS. So like any entity, it is all about prioritization for us. So we spend a lot of time figuring out with finite resources, even with growth, with finite resources how are we going to prioritize.

So our input for the fiscal year 2018 budget in truth in lending, we just rolled it out as a government, as a Department this afternoon, during the midday today, so I have not yet seen the specifics yet. I know what the broad number for us is, but I haven't seen the sub-elements of that, so I will talk broadly. I apologize, but I will talk broadly.

For the 2018 input, we tried to identify those priorities. At a macro sense, in no particular order, I have been arguing manpower; investment in core capabilities; and then, number three, how can I accelerate number one and number two, how can I do both of those faster.

Because in some ways, even though as the WannaCrypt ransomware issue that we have been going through shows, there is capability in the Department. There are a lot of motivated men and women who are doing some good work. We were not impacted by WannaCrypt, and that wasn't from a lack of effort.

We had spent significant time starting in March asking ourselves how might this play out, how do we position ourselves in the case of—because Microsoft had put out the patch for the vulnerability. We, as Microsoft users, saw that and started asking ourselves how might an opponent attempt to exploit this vulnerability even as we were working to patch.

It is one of the reasons why we use a defense in-depth strategy. There is no one single solution. There is no one single way to fix this problem. It is layers built on top of each other. That really has been the key to our success.

So we are asking ourselves how can we do this faster. Every day, one of my biggest concerns is—and I have never really had this same viewpoint in almost 36 years of commissioned service—every day I literally think to myself, we are in a race to generate more capacity and more capability at the same time that I am watching a host of global actors do the exact same thing.

And so we are trying to sustain both staying up with them, but, quite frankly, my objective is to get ahead of the problem set. I don't like reacting to things. It is not an effective or efficient way to do business, and I don't think that is what the Nation wants from us.

So until I am able to bore into the specifics of the budget, that kind of gives you a broad sense of what I thought we needed to focus on.

Ms. CHENEY. So would you say, Admiral, that the budget as it has been proposed provides the resources necessary to regain superiority in areas that we have lost it?

Admiral ROGERS. It certainly moves us along that road, but no one should think for one moment that this mission set, not unlike some others, is going to require increased and sustained investment over time. This is not going to be a 1 or 2 years we have increased you by some reasonable number, which has been the case for the last 2 years, and that is all you are going to need.

If you look at the scope of the challenges associated with this mission set and from where we are starting, we have got a lot of hard work ahead of us.

Ms. CHENEY. And would you talk a little bit about how you are going to measure success and how you are going to measure progress along that path of regaining superiority?

Admiral ROGERS. So there are a couple components to it. First, we have developed a set of—we are in the process of developing a set of metrics, so how do we truly assess readiness for this force that we created.

We focused for the first few years on assessing initial operating capability [IOC] and final operating capability [FOC]. It is when you hear us talk in slang about IOC and FOC. And you heard me in my remarks, we achieved IOC essentially on time, October 2016. We have until 30 September, 2018, to achieve FOC. I think we are on track for that.

But one of the things I tell the team is that doesn't get to warfighting. And in the end, it is about our ability to actually operate in a sustained heavy environment. Just like when we are building a brand new carrier or a brand new fighter wing, for example, it is not enough just to say we have got all the pilots, we have got all the parts. It is about training. It is about assessing readiness. So we are working our way through how are we going to do that.

Then it is other things like we ask ourselves are we driving down defensive penetrations, are we driving down malware infections. There are some specific metrics that we think that we can use to give us a sense, particularly on the defensive side, are we being more effective or not.

Ms. CHENEY. Thank you very much. My time has expired.

Ms. STEFANIK. Mr. O'Rourke.

Mr. O'ROURKE. Thank you.

Help me understand a little bit how we make clear to other countries in the world the consequences of cyber attacks. With conventional weapons in conventional wars there may be an understanding of what the consequences will be should one country attack another with a certain kind of weapon. What is our level of dialogue with other countries, including those countries we view as threats, including those countries who, I think, we know who have attacked us, about what the consequences are going forward?

Admiral ROGERS. So if I could in an unclassified session, I am not going to get into specifics associated with particular nation-states. And it hasn't been a one-size-fits-all approach, which is true broadly for strategy for us, I would argue, as a Nation. It is not a one-size-fits-all approach. We try to optimize the way we are looking at this particular challenge set based on whatever the particular actor that we are dealing with. What works for one won't necessarily have the same kind of impact as what will work for another.

There are a couple—first, let me talk about a couple basic things. We have been very public and acknowledged the fact that we are using cyber offensively against ISIS, not just because we want ISIS to know that we are contesting them, but because, quite frankly, we also think it is in our best interest for others to have a level of awareness that we are investing in capability. And we are employing it within a legal Law of Armed Conflict framework, not indiscriminately, but we are employing it.

We have also acknowledged very publicly in unclassified strategy documents, for example, for the Department's cyberspace strategy, that we are developing offensive capability, that we believe that deterrence is an important concept that we have got to work our way through. We are trying to communicate to the world around us that we are aware of the kinds of activity we are seeing out there. Some of it we view with concern.

As a result, we think it is in our own Nation's best interest to have a set of capabilities that both generate greater options for our policymakers and our operational commanders, but at the same time help communicate to others around us you don't want to go down this road with us.

I think the reaction or the way WannaCrypt played out in the United States, for example, is a very good example of that. Hey, look, in a major malware effort that took down many systems in lots of other parts of the world, did not have the same level of effect on us here in the United States. That is not by chance.

Mr. O'ROURKE. Let me ask you a question about that. To what degree are we treaty bound to assist an ally who is attacked through cyber not kinetically, and are we already assisting allies who are? And maybe to use that most recent example that you just gave.

Admiral ROGERS. So that is a bit of a legal question. That is not my lane. But I will give you my thoughts from my perspective as an operational commander.

For example, NATO has been very direct in saying that they view cyber as a natural continuation of the standing Article 5 framework where attack against one is an attack against all, even as NATO acknowledges the application of Article 5 is through a decision framework in the North Atlantic Council, and it is done on a case-by-case basis. But broadly that is the intent. That has been communicated in multiple forms, in multiple ways.

For other nations, you would have to ask somebody who is a little bit smarter about the specifics of the standing mutual defense treaties that we have.

Mr. O'ROURKE. Okay. Let me ask another question then. Because we know the Russians attacked the integrity of our elections here, because we know they have done that in other countries, because past behavior is a good predictor of future behavior, whose responsibility is it in this country? And then maybe for the record on for our allies when our allies' elections are attacked.

But is it Cyber Command? Is it DHS? Is it both? Should the RNC [Republican National Committee] or the DNC [Democratic National Committee] be attacked going forward, for example, whose responsibility is that?

Admiral ROGERS. So under the current framework, which could change, but under the current framework the Department of Homeland Security has overall responsibility for the provision of capability and capacity within the Federal Government in support of the private sector, broadly.

Cyber Command in its defined mission of, if directed, as I said, to support the defense of critical infrastructure, we would partner with DHS to do that. We would do that, Cyber Command, by attempting to interdict that activity before it ever reached that U.S. network. Quite frankly, we wouldn't focus on blue or friendly space. We would be out in gray and red space, if you will, trying to stop the activity from ever getting there.

Mr. O'ROURKE. It is yours before it gets here. Once it gets here, it is DHS.

Admiral ROGERS. Yeah, simplistically. Then once it gets here, DHS has created a sector framework. Cyber Command also has a set of capabilities in the form of national cyber protection teams that we would also deploy in partnership with DHS to support among those 16 specific critical infrastructure areas.

Again, it is one of the things I mentioned earlier that I want to test. We are going to start using one particular sector that is a little bit more mature than some of the other 15.

Mr. O'ROURKE. Thank you.

Ms. STEFANIK. Mr. Franks.

Mr. FRANKS. Well, thank you, Madam Chair. And thank you, Admiral Rogers. Thank you for your service to the country, and your job is so very important to us all.

You stated that your first mission priority is defense of DOD information networks. Would you suggest that that means that defensive operations doctrinally will take precedence over offensive operations?

Admiral ROGERS. No, because I remind the team: Look, we have three missions, and we have to be capable of executing all of them. I can't go to my boss and say: Hey, I really just chose to focus on number one.

Now, don't get me wrong. Like any commander, I have to prioritize. And so as I am looking at the challenges out there, I have told the team we will prioritize against number one, even as we acknowledge we still have to execute those other two missions.

But like any other operational organization, at times I have to prioritize resources, focus. But it isn't: Well, it is just one and not the others. We have got to do all of them.

Mr. FRANKS. Yeah. Well, as you know, the DOD relies upon the civilian power grid for 99 percent of its power requirements, without which, I am told, that it becomes impossible in CONUS [continental United States] to effect the DOD mission. Do your priorities include protecting the U.S. power grid and other critical infrastructure against cyber attacks?

Admiral ROGERS. So, again, I don't have responsibility for the defense of that in the United States.

I will say, one of the things I am interested to see if we can maybe look at doing differently, and I am having this conversation in particular with TRANSCOM [Transportation Command] at the moment, right now, when it comes, for example, to critical infra-

structure that the DOD counts on to do its mission, when it comes to cleared defense contractors who either are generating the capabilities that we use, advanced fighters, for example, and other platforms, as well as private industry, for example, for TRANSCOM that provides services, lift, movement of cargo, under the current structure the Defense Security Service [DSS] has overall responsibility for the interface with those private companies, not TRANSCOM, for example, even though they work for TRANSCOM or they provide a service based on a contractual relationship with TRANSCOM, and not necessarily with us.

I would like to see, is there a way to bring those operational commands, Cyber Command, DSS, and that private sector together in a much more integrated way, because what we are finding right now is I will become aware of activity, I will pass that to DSS, DSS passes that to the private sector. That doesn't come across to me always as the fastest, most efficient, most agile way to do business, and I would like to see if we can maybe try to change that.

Mr. FRANKS. Well, Admiral, you know that that has been one of the challenges in the past, that sometimes the whole notion of protecting the grid from cybersecurity challenges kind of walks the 13th floor of humanity.

Admiral ROGERS. Right.

Mr. FRANKS. Because we, the Department, your department consider that a civilian responsibility. Of course, the civilian response is that that is a national security issue and should not be our responsibility. And my fear, of course, is that neither has the sufficient focus on it necessary. And given it is your stated——

Admiral ROGERS. Yes, sir.

Mr. FRANKS. Yeah. So it is worth always touching base on.

How will Cyber Command's posture improve once it is elevated? Do you believe you will have all the resources and authorities you require to accomplish your assigned missions? And what do you expect your number one challenge will be in terms of Russia, China, Tehran, ISIS, someone else?

Admiral ROGERS. Okay. So let me try to unpack it, and if I forget one, please just let me know, sir.

So first, what is the benefit of elevation, why have I and others recommended that that is a smart course of action, even as I acknowledge the decision is not mine, as we have already talked? That is outlined within legislation. Now it is a timing issue absent a change to the legislation.

In the Department's processes, when it comes to how we develop budgets, how we articulate prioritization, how we develop broad policy, it is generally built around the idea that the combatant commanders are the primary voices for the operational end of those processes, not subunified commands, combatant commanders.

So one of my concerns has been we talk about the importance of cyber—and I acknowledge that there are other priorities in the Department—and yet, for some—not all but for some of our processes the cyber expertise is not embedded in the current structure because you put it one level below.

So I believe that elevation plugs us more directly into the primary decision-making processes within the Department, which are really optimized for combatant commanders. It also makes us fast-

er, because now I have got one less layer that I have to work through. I have been very blessed in my time at Cyber Command.

The Strategic Command commanders I have worked with, General Hyten and—boy, how quickly we forget, I can picture, he was a good flag officer, a friend—they were great to team with, because I would tell them: Look, if we are going to insist everything I do flows through Offutt [Air Force Base], I can't get to timeliness, I can't get to speed. And this helps address that.

Ms. STEFANIK. The time has expired.

I now recognize Mr. Cooper.

Mr. COOPER. Thank you, Madam Chair.

Apparently, two of our colleagues have introduced a bill that would allow private sector U.S. companies to hack back, active defense. I hadn't realized before that this is apparently illegal today absent a law change. So could you reflect on this proposal and whether it is a good idea or not?

Admiral ROGERS. So broadly—and I will only speak for Mike Rogers, because I am not in the policy lane but I have an opinion—as an operational commander, my concern is while there is certainly historic precedence for this, nation-states have often gone to the private sector when we lacked government capacity or capability.

We did that in the Revolutionary War, letters of marque. We didn't have a Navy. We went to the private sector, gave them authority and protection via our government to say go out and capture cargos from the Royal Navy and from the British merchant fleet.

My concern is, be leery of putting more gunfighters out in the street in the Wild West. As an individual tasked with protecting our networks, I am thinking to myself, we have got enough cyber actors out there already. Just putting more out there I am not sure is in everybody's best interest.

And I would also be concerned about the legal liability you might—and I am not a lawyer—about the legal liability. I would think that you would have some liability issues associated with taking actions with second- and third-order effects that you don't truly understand when you actually execute it. That is just my concern.

Mr. COOPER. Are other countries doing this? Are you familiar with any other countries that have enabled their private sector to be aggressive?

Admiral ROGERS. There may be equivalent legal frameworks out there, certainly not that have come to my attention and not that I have a discussion about.

Mr. COOPER. I was curious, you used a gunfighter analogy, because some people have thought that NRA [National Rifle Association] might set up a whole new wing of activity for this.

But to the extent that private business in this country feels disconnected from government or that, as you pointed out earlier, government response is too slow or that certain national security interests are not recognized as being national security interests even when it is protecting the grid, I think you are probably going to see greater pressure.

Admiral ROGERS. Right. I would agree.

In some ways, it goes back to—again, showing you my war college education. I don't want you to think as a taxpayer I didn't listen when I was sent to service colleges.

In the Westphalian construct, the application of force has generally, for the last several centuries, been viewed as a mission or a right of a sovereign state, not something that the private sector does. We don't use, for example, for us, we don't use contracts to actually drop and fire weapons. We don't use mercenaries to do that. We use uniformed military.

I would just be concerned that going that route, again, argues against the broad principles we have used about the role of the state and applying force kinetically or nonkinetically.

Mr. COOPER. We don't use those tools, but in our degraded Westphalian system, we don't know who we are being attacked by. It might be state actors, quasi-state actors, probably private actors. Who knows?

Admiral ROGERS. Although it depends on the situation. But I am the first to acknowledge 100 percent attribution is probably a standard we are going to be driving for for a long time and not necessarily achieve immediately.

Mr. COOPER. What percentage of accuracy in attribution would you give us today?

Admiral ROGERS. Oh, it depends on the actor. If you take, for example, speaking now on the NSA side, if you take a look at the efforts we did in the intelligence community assessment with respect to Russian efforts to influence the 2016 election process, really high confidence, very fine-grain attribution.

If you take a look at WannaCrypt, for example, we are 10 days into this, and collectively, both the private sector and the government, we are still working our way through who is the actor or actors associated with this. So it tends to vary. There is no single concrete answer.

Mr. COOPER. So with the elections, we are close to 90 percent, 95 percent, and with this we are 60 but raising it?

Admiral ROGERS. I don't know. I have never really thought about it from a number.

Mr. COOPER. Okay. Thank you, Madam Chair.

Ms. STEFANIK. Mr. Scott.

Mr. SCOTT. Thank you, Madam Chair. Admiral, it is a long way from Auburn University.

Admiral ROGERS. War Eagle, sir.

Mr. SCOTT. I hope you never lose a war or win a ball game. I am University of Georgia graduate.

Admiral ROGERS. Oh, I have a brother who went to the University of Georgia and a sister-in-law.

Mr. SCOTT. He is a good man. He is a good man.

Admiral ROGERS. Misguided individuals. I love them, but they are misguided.

Mr. SCOTT. Was he the one holding Uga when he bit the Auburn player?

All kidding aside, thank you for your service.

And we talk a lot about how fast technology changes and the acquisition process being a problem throughout the Department, but

I would like to hear your comments on the personnel again. You speak to this in your comments.

When you get the young man, the young woman out there that is the best and the brightest, there are opportunities in the private sector versus there are opportunities in the public sector under your command. The challenges there. And the issue of, what percentage of your personnel are civilian versus uniform?

Admiral ROGERS. Roughly, we are about 80 percent military, about 20 percent civilian. That is kind of what we are building to. It varies in some areas, but it is about 80–20.

Mr. SCOTT. I know we have a tremendous number of wonderful people in uniform. Some of the people that we see that seem to be the best and the brightest in the technology field aren't exactly the people that you imagine going to boot camp.

Admiral ROGERS. Right.

Mr. SCOTT. How do we recruit in case—I mean, do we have a system in place to allow those people to serve?

Admiral ROGERS. So it is one of the reasons why we have tried to come up with a total force concept for us—Active, Guard, Reserve, civilian, contractor—that within that pool of five subpopulations, if you will, we can match almost any individual.

"Hey, I really want to get into this. I want to serve the Nation. But I have no desire to deploy or be put through the physical fitness standards of the uniform law. Boy, I would love to work for you as a civilian."

"Hey, I like mobility, I am going to try the contractor route so I can move around a little bit."

We try to build a structure that enables us to try to attract a pretty broad swath.

The positive side to me is, boy, when you get people in the team—I was just talking to one of the service review panels. One of the services out there has created—has asked a party of gray beards to take a look at how they manage the Cyber Mission Force within their service and to answer the question: Are they really optimized for the future?

And I coincidentally this morning was just sitting down with this retired former chief of their service. And I said, "Well, you have talked to the teams," because they did that as part of their process. I said, "Tell me what you are hearing from them, because I have a sense, but I am curious what you are hearing."

And he said to me, "The most amazing thing is every team we talk to, these men and women are so motivated and love what they are doing. I mean, that is a real plus for you. They really are into this mission. Because their self-image is they are the digital warriors of the 21st century."

The challenge, I think, we have got to work with the services who provide this manpower capability, how do we manage it effectively over time, and how do we also build into this the fact that we have got to acknowledge there are some areas we are going to need to do differently? We can't put a person in this once and then spend all that time training him and then they don't do it for another 10 years. That is ridiculous to me.

On the other hand, I realize that there is more than just the Cyber Mission Force, that the services are asking themselves: How are we building a broader workforce to address cyber?

So I am working with the services about what percentage of the eligible trained population makes sense, what kind of policies we should have with respect to retouring them so we sustain some level of capability and experience over time and we are not starting all over again every 3 years.

That is one of the challenges at the moment that one service is trying to deal with. Their model, I am trying to argue, we have got to make some changes to. We just can't afford to retrain everybody every 3 years. I just don't think that is cost effective, and it is a little demoralizing to the men and women.

Mr. SCOTT. I think this is going to be one of our greatest challenges going forward in how we handle the cyber war, if you will.

Admiral ROGERS. Right.

Mr. SCOTT. And not just with your issue. We hear the same thing about the drone pilots and how dedicated they are and how determined they are and the need for flexibility——

Admiral ROGERS. Yes, sir.

Mr. SCOTT [continuing]. With where they work and the time that they work. And I recognize, from a pay scale, we are nowhere close to what they would get in the private sector.

Admiral ROGERS. Right. But on the other hand——

Mr. SCOTT. So I appreciate their commitment to the country and your commitment to the country as well.

Thank you.

Ms. STEFANIK. Mr. Wilson.

Mr. WILSON. Thank you, Chairwoman Elise Stefanik, for your extraordinary leadership on organizing this hearing.

And it is just an honor, Admiral, to be back with you, and we appreciate your innovative service to address the issues of cyber defense.

As the former chairman of the Subcommittee on Emerging Threats and Capabilities, I am keenly aware of the huge challenges that lie before us and the extraordinary men and women that you have put together to serve in your command.

Cybersecurity is a 24-hour-a-day, 365-day-a-year responsibility that requires instantaneous analysis, response, and deterrence. After each cyber attack, we have the circumstance of where the government officials are grappling with whether or not it constitutes a mere nuisance or an act of war.

It is for this reason I introduced the Cyber Attack Standards of Measurement Study Act, H.R. 1030, which would require the Director of National Intelligence, the Homeland Security Department, FBI [Federal Bureau of Investigation], and Secretary of Defense to conduct a study to determine appropriate standards that could be used to quantify the damage of cyber incidents for the purpose of determining appropriate response.

And two questions. Do you believe that there exists an interagency definition for cyber act of war? And secondly, do you believe that we have a common metric to measure cyber incidents which could benefit the interagency response?

Admiral ROGERS. I think there is a broad, certainly in the kinetic world, there is a broad definition out there of an act of war. But even in the kinetic world, it is still somewhat situational. And so I fully expect that our experience in cyber is going to be something similar.

It goes to one of the previous questions in some ways. Articulating those concepts in a way that actors understand that you may be tripping a threshold that will trigger a response, I think that is in our best long-term interest. That helps, I think, help the nation-states, actors, groups out there understand there are potential prices to pay here, and at some point you will trip a threshold—again, depending on the scenario—and that is not a good place for you to be.

We are clearly still working our way through there. And I am not a policy guy, I am the operational guy, so I try to figure out what do we do once the policymaker makes that determination.

Mr. WILSON. And then thank you for recognizing, too, it could be nation-states, it could be other actors. What a challenge. And so we are so grateful for your service.

One of the first challenges that you have are updating antiquated infrastructure.

Admiral ROGERS. Yes, sir.

Mr. WILSON. I am grateful that the district I represent is adjacent to Fort Gordon, home of the Army Cyber Command. Can you please describe the amount of infrastructure modernization that needs to occur and how the demand differs across the Army, Navy, Air Force, and Marines?

Admiral ROGERS. So as we saw—and I will use WannaCrypt as an example—as we are working our way through the services, because I have overall operational responsibility, the services physically own much, under the current network structure, the services still own much of the infrastructure. So I partner with them in attempting to address that infrastructure cybersecurity.

One of the things we continue to find is we are still carrying a lot of very old infrastructure that offers potential increased vulnerability. And the "defense in depth" approach we use is designed to help mitigate that, but I literally just sent a note to a service chief earlier this week and senior leaders in that service and said: Look, at some point these vulnerabilities down at the tactical level that interact with acquisition will become potential points of exploitation by others that have the chance to negate some of that defense in depth. So we have got to address this.

I find we have talked a lot about manpower, but in some ways, to me, the acquisition piece, that is even harder, because it is long term, it is huge sunk cost, and it is competing against priorities like: So do you want me to buy more F–35s? Additional, you know, carriers? Do you want more brigade combat teams?

In a world of finite resources, you have got to make those resource tradeoffs, and, in general, the acquisition world hasn't historically always been incentivized for cybersecurity outcomes as its primary metric.

Mr. WILSON. Well, thank you very much. And we look forward to working with Chairwoman Stefanik to back you up in every way.

Admiral ROGERS. Thanks.

Mr. WILSON. And with my time running out, I do want to thank you for the participation by the National Guard and your efforts. And what has been the level and what more can we do to help you in this regard?

Admiral ROGERS. Boy, so if we just look at Cyber Command, we have over 100 guardsmen and reserves every day supporting us. Every day we currently have Guard components activated on the defensive side, on the offensive side, in some of our specialized capabilities. So the Guard is a day-to-day player for us.

If you also look at what the Guard is doing from an—oops, sorry ma'am.

Mr. WILSON. Thank you very much.

Ms. STEFANIK. Time has expired. They are calling votes, and so I want to get to everybody.

Dr. Wenstrup.

Dr. WENSTRUP. Thank you, Madam Chair. Admiral, good to be with you here today. I appreciate it.

You were talking about various structures of how we set up our command and where we are headed. I am curious what our adversaries are doing. What do we know about how they are structured and looking at what they are doing and maybe guiding us in some way?

Admiral ROGERS. In some ways, it is kind of interesting. Again, I am not going to get into a classified discussion. But broadly, Cyber Command is viewed as: Wow, this is a really interesting concept that the U.S. has created, what can we do to attempt to emulate at least parts of it?

I am not arguing that it is perfect or that everyone else in the world wants to. But, in general, I spend a lot of time talking to allies, and they will often say to me: Well, we may not opt to go the same particular structure you have created, the process you went through, the capabilities you have developed, the way you have created an organizational operational construct that is focused on generating outcomes, hey, we are really interested in doing that. Is there a way we can potentially partner?

So part of the Cyber Command's mission set right now is you spend a lot of time with foreign partners around the world. And I can't—I am the first to acknowledge I have to prioritize here, but as part of the broader Department strategy, I have prioritized different areas of the world that we are really heavily focused on right now in terms of partnership, helping those nations develop cyber capability.

Dr. WENSTRUP. That is our allies. And you mentioned, in a different setting, go into more detail what our adversaries are——

Admiral ROGERS. Right. If I could, I would be glad, in a closed session and share some interesting thoughts there.

Dr. WENSTRUP. Another time. That is fine. I appreciate that.

You did mention that we wanted people to know some of the things we were doing to counter ISIS, and maybe that is kind of hitting them, but a shot across the bow for others. Have you felt that it has had an effect?

Admiral ROGERS. I certainly hope so, because, quite frankly, again, one of the reasons we opted to publicly acknowledge this was we wanted other actors to be aware that we are developing

and employing—again, within a legal framework—but we are developing and employing those capabilities.

There certainly is an increased awareness by some actors around the world as they look at us, as they try to study us, about capabilities and kinds of things we are doing. Again, I am not going to get into specifics, but we are certainly aware of that.

Dr. WENSTRUP. Yeah, in another setting I might like to hear more about that.

Admiral ROGERS. Yes, sir, I would be glad to.

Dr. WENSTRUP. Yeah, we will have that opportunity, I am sure. Thank you very much. I yield back.

Admiral ROGERS. Yes, sir.

Ms. STEFANIK. Thank you.

Thank you very much, Admiral Rogers, for your testimony.

At this time, they are likely to call votes in the next couple of minutes or so. After votes are finished, we will reconvene in Rayburn 2337 upstairs for the closed portion of this.

If there are additional questions from the members, please feel free to submit them for the record, and then we can anticipate a response from you.

Admiral ROGERS. Yes, ma'am.

Ms. STEFANIK. This committee is adjourned, and we will reconvene.

Admiral ROGERS. Thank you, ma'am.

[Whereupon, at 4:46 p.m., the subcommittee proceeded in closed session.]

A P P E N D I X

MAY 23, 2017

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

MAY 23, 2017

Opening Statement
Chairwoman Elise M. Stefanik
Emerging Threats and Capabilities Subcommittee
Fiscal Year 2018 Budget Request for U.S. Cyber Command: Cyber Mission Force Support to Department of Defense Operations
May 23, 2017

The subcommittee will come to order.

I want to welcome everyone to today's hearing of the Emerging Threats and Capabilities Subcommittee of the House Armed Services Committee. With the President's budget request released just earlier today, this is our first opportunity to explore this request and the major implications for key defense missions. I think it is fitting that the first area we will dive into is cyber. This is an increasingly important domain of warfare, and an area where we have increased our emphasis on overseeing the Department's progress in building and maintaining cyber forces to protect, defend, maintain, and when necessary, conduct offensive operations in cyberspace.

As we move towards developing the Fiscal Year 2018 National Defense Authorization Act, I have made cyber and cyber warfare one of my main priorities. In the coming weeks, Chairman Mac Thornberry and I, in addition to my ranking member Jim Langevin and the HASC Ranking Member Adam Smith, plan to introduce stand-alone cyber warfare legislation that strengthens Congressional oversight of sensitive military cyber operations, including mandating prompt notifications to Congress in the event of unauthorized disclosures. We look forward to continuing to work with U.S. Cyber Command and the Department of Defense as we finalize this draft legislation to ensure such notifications are responsive to our needs, but without adding undue reporting burdens on the Department of Defense.

In addition to our focus on strengthening Congressional oversight in the area of cyber warfare, other key focus areas will include provisions to strengthen our own cyber warfare capabilities, and provisions that enhance our international partnerships across the globe.

In order to more thoroughly understand all of these issues, I would like to welcome our witness today—Admiral Michael Rogers, who serves as the Commander of U.S. Cyber Command and the Director of the National Security Agency.

I would also like to remind members that immediately following this open hearing, the committee will reconvene upstairs in 2337 for a closed, classified Roundtable discussion with our witness.

Admiral Rogers, we have much to discuss, and we look forward to your testimony. The floor is yours.

STATEMENT OF

ADMIRAL MICHAEL S. ROGERS

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

HOUSE COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

23 MAY 2017

Chairwoman Stefanik, Ranking Member Langevin, and Members of the Subcommittee, 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

[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.

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 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.

Admiral Michael S. Rogers
Commander, U.S. Cyber Command
Director, National Security Agency
Chief, Central Security

Admiral Michael Rogers is a native of Chicago and attended Auburn University, graduating in 1981 and receiving his commission via the Naval Reserve Officers Training Corps. Originally a surface warfare officer (SWO), he was selected for re-designation to cryptology (now Information Warfare) in 1986.

He assumed his present duties as commander, U.S. Cyber Command and director, National Security Agency/Chief, Central Security Service in March 2014.

Since becoming a flag officer in 2007, Rogers has also served as the director for Intelligence for both the Joint Chiefs of Staff and U.S. Pacific Command, and most recently as commander, U.S. Fleet Cyber Command/U.S. 10th Fleet.

Duties afloat have included service at the unit level as a SWO aboard USS Caron (DD 970); at the strike group level as the senior cryptologist on the staff of commander, Carrier Group 2/John F. Kennedy Carrier Strike Group; and at the numbered fleet level on the staff of Commander, U.S. 6th Fleet embarked in USS Lasalle (AGF 3) as the fleet information operations (IO) officer and fleet cryptologist. He has also led cryptologic direct support missions aboard U.S. submarines and surface units in the Arabian Gulf and Mediterranean.

Ashore, Rogers commanded Naval Security Group Activity Winter Harbor, Maine (1998-2000); and, has served at Naval Security Group Department; NAVCOMSTA Rota, Spain; Naval Military Personnel Command; Commander in Chief, U.S. Atlantic Fleet; the Bureau of Personnel as the cryptologic junior officer detailer; and, Commander, Naval Security Group Command as aide and executive assistant (EA) to the commander.

Rogers' joint service both afloat and ashore has been extensive and, prior to becoming a flag officer, he served at U.S. Atlantic Command, CJTF 120 Operation Support Democracy (Haiti), Joint Force Maritime Component Commander, Europe, and the Joint Staff. His Joint Staff duties (2003-2007) included leadership of the J3 Computer Network Attack/Defense and IO Operations shops, EA to the J3, EA to two directors of the Joint Staff, special assistant to the Chairman of the Joint Chiefs of Staff, director of the Chairman's Action Group, and a leader of the JCS Joint Strategic Working Group.

Rogers is a distinguished graduate of the National War College and a graduate of highest distinction from the Naval War College. He is also a Massachusetts Institute of Technology Seminar XXI fellow; Harvard Senior Executive in National Security alum; and holds a Master of Science in National Security Strategy.

Updated: 20 November 2014

QUESTIONS SUBMITTED BY MEMBERS POST HEARING

MAY 23, 2017

QUESTION SUBMITTED BY MS. STEFANIK

Ms. STEFANIK. I am aware that staff from the legislative branch have been participating in DOD's Cyber Guard exercise series over the past 2 years in an effort to better defend our own networks. Cyber Guard helps to prepare for a major cyber event by training for a whole of nation approach led by DOD, DHS, FBI, with private sector participants for CI/KR sectors and the legislative branch. Are there other training opportunities that would make sense for the legislative branch to participate in, such as other Continuity exercises or smaller scale cyber technical or operational training?

Admiral ROGERS. [The information was not available at the time of printing.]

QUESTIONS SUBMITTED BY MR. LANGEVIN

Mr. LANGEVIN. The Fiscal Year 2017 National Defense Authorization Act also formalized the relationship between the Principal Cyber Advisor and CYBERCOM to establish a service-like secretary. A service-like secretary is critical for advocacy and oversight of the command and for ensuring operations are synched with policies, as well as civilian control of the military. In light of the law, what steps has CYBERCOM taken to enhance the relationship between OSD and the command?

Admiral ROGERS. [The information was not available at the time of printing.]

Mr. LANGEVIN. The Persistent Training Environment is key to a ready force. What is the status of the effort based on funding provided to date? What can we expect in FY18 both in funding and capability delivery?

Admiral ROGERS. [The information was not available at the time of printing.]

Mr. LANGEVIN. The military services are making significant investments in cyber training and cyber centers of excellence. Although I'm pleased to see the investment, I want to ensure coordination and avoid duplicative efforts. How are you encouraging the services to leverage respective centers of excellence, and investment in training generally?

Admiral ROGERS. [The information was not available at the time of printing.]

Mr. LANGEVIN. Academia and industry have much to offer the Department of Defense in the cyber domain, from strategic thinking to experienced personnel to technology. Please describe the relationships CYBERCOM has with academia and industry. How have these relationships benefited the Department?

Admiral ROGERS. [The information was not available at the time of printing.]

QUESTIONS SUBMITTED BY MR. FRANKS

Mr. FRANKS. You stated your first mission priority is defense of DOD information networks. Will defensive operations doctrinally take precedence over offensive operations?

The DOD relies on the civilian power grid for 99% of its power requirements. Do you believe your priorities include protecting the U.S. power grid and other critical infrastructure against cyber attacks?

Admiral ROGERS. [The information was not available at the time of printing.]

Mr. FRANKS. How will Cyber Command's posture improve once elevated: Do you believe you will have all the resources and authorities you require to accomplish your assigned missions?

Who do you expect your #1 challenge to be? Russia, China, Iran, ISIS, someone else?

Admiral ROGERS. [The information was not available at the time of printing.]

Mr. FRANKS. In your opinion, what are we missing in our thinking to get to an effective comprehensive approach that allows for deterrence and rapid response capabilities?

What do we know about the cyber doctrine and military structure of our adversaries and allies?

While we may have some sense of Russian and Chinese actors, do we have any understanding of other actors and has doctrine been established to counter threats from them (Syria, Iran, Israel, Germany, etc.)?

Admiral ROGERS. [The information was not available at the time of printing.]

QUESTIONS SUBMITTED BY MRS. MURPHY

Mrs. MURPHY. I am encouraged that the Department is moving forward on creating the Persistent Cyber Training Environment, which will be a training platform to allow cyber forces to train in simulated network environments. The Army's Program Executive Officer for Simulation, Training, and Instrumentation (PEO STRI), based in Orlando, was tapped as the lead to develop and acquire the Persistent Cyber Training Environment, which will also incorporate the work of the National Cyber Range in Orlando.

In your view, what is the value of the Persistent Cyber Training Environment for readiness? What individual and collective training gaps will the Persistent Cyber Training Environment fill?

Admiral ROGERS. [The information was not available at the time of printing.]

Mrs. MURPHY. Earlier this year the Committee heard from LTG Joseph Anderson (Deputy Chief of Staff, G–3/5/7) that our commanders don't have the facilities or capabilities to understand what cyber does for them, both from a defensive and offensive perspective.

How might the Persistent Cyber Training Environment help increase cyber fluency at leadership levels in the Army, and across the services?

Admiral ROGERS. [The information was not available at the time of printing.]

Mrs. MURPHY. You stated in your testimony that CYBERCOM is working to synchronize cyber planning and operations across the joint force, and that CYBERCOM is helping the combatant commands build cyber effects into their planning processes. How exactly is CYBERCOM doing this?

Admiral ROGERS. [The information was not available at the time of printing.]