[H.A.S.C. No. 115–97]

HEARING

ON

NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2019

AND

OVERSIGHT OF PREVIOUSLY AUTHORIZED PROGRAMS

BEFORE THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES
ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES HEARING

ON

A REVIEW AND ASSESSMENT OF THE DEPARTMENT OF DEFENSE BUDGET, STRATEGY, POLICY, AND PROGRAMS FOR CYBER OPERATIONS AND U.S. CYBER COMMAND FOR FISCAL YEAR 2019

HEARING HELD
APRIL 11, 2018

U.S. GOVERNMENT PUBLISHING OFFICE
30–571 WASHINGTON : 2019

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
DOUG LAMBORN, Colorado
AUSTIN SCOTT, Georgia
JODY B. HICE, 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

PETE VILLANO, *Professional Staff Member*
LINDSAY KAVANAUGH, *Professional Staff Member*
NEVE SCHADLER, *Clerk*

CONTENTS

A REVIEW AND ASSESSMENT OF THE DEPARTMENT OF DEFENSE BUDGET, STRATEGY, POLICY, AND PROGRAMS FOR CYBER OPERATIONS AND U.S. CYBER COMMAND FOR FISCAL YEAR 2019

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES,
Washington, DC, Wednesday, April 11, 2018.

The subcommittee met, pursuant to call, at 3:30 p.m., in room 2212, 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.

Welcome, everyone, to today's hearing of the Emerging Threats and Capabilities Subcommittee on the posture of cyber operations and U.S. Cyber Command [CYBERCOM] for fiscal year [FY] 2019.

This hearing is the second of three cyber events today. This morning, we heard from former Secretaries of Homeland Security Chertoff and Johnson, as well as former CYBERCOM Commander Keith Alexander.

Adversaries such as China and Russia aggressively leverage and integrate cyber information and communications technologies for geopolitical and economic gain, and they do so in a seamless way. Dictatorships have those advantages, and their control over these technologies and information is as much about exerting control over their own populations as it is confronting free societies such as ours.

As discussed in the Worldwide Threat Assessment for 2018 from the Director of National Intelligence [DNI], Iran and North Korea also continue to increase their offensive cyber capabilities and techniques. Over the last few years, both of these nations are believed to be behind cyber attacks that demonstrate not only a capability to deploy a variety of techniques and tools, but also a willingness to use cyber attacks as a means to achieve their national objectives.

Needless to say, cyber threats today from state and non-state adversaries are real, pervasive, and growing. Cyberspace and the information domain writ large remains contested and under continual stress. We are no longer peerless, and cyber superiority is not assured.

Yet, while these adversaries continue to use cyber as a means to achieve strategic objectives, I remain concerned that we, as a government, do not have a strategy in place to mitigate, deter, or op-

pose their advances. It is safe to say that we have improved our military cyberspace and cyber warfare capabilities and also improved our resilience in many areas, but I am sure not the same can be said of the rest of our government—most notably, the protection of our critical infrastructure that preserves our economic security and ensures our way of life.

Further work is needed to build interagency partnerships to ensure a whole-of-government approach to countering the growing cyber threat. The Department of Defense [DOD] plays an important role in this area, certainly when considering a significant cyber incident that may require their expertise during a time-sensitive emergency.

From where I sit, a great deal of work remains to be done to improve our ability to defend, fight, and win in this critical domain, and also to improve and align our decision-making processes and operational authorities so that we are fast, agile, and relevant. Only then will our Nation be prepared for the 21st-century challenges we face.

Our witnesses today are very well-qualified to help us navigate these multidimensional challenges. Appearing before our subcommittee, we have Admiral Mike Rogers, Commander of U.S. Cyber Command and Director of the NSA [National Security Agency], and the Honorable Kenneth Rapuano, Assistant Secretary of Defense for Homeland Defense and Global Security and Principal Cyber Advisor for the Secretary of Defense.

Thank you both for being here today.

Admiral Rogers, this will be your last appearance before this subcommittee, and I want to extend my sincerest thanks and appreciation for your decades of service to our country and for the relationship that you have built with so many of our members on the House Armed Services Committee [HASC]. We wish you great success in your next chapter and wish your family well. Thank you again for your service.

I would now like to recognize my friend and the ranking member, Jim Langevin, for his opening remarks.

[The prepared statement of Ms. Stefanik can be found in the Appendix on page 25.]

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

Mr. LANGEVIN. Thank you, Chairwoman Stefanik.

And thank you to both of our witnesses for being here today. I look forward to your testimony. I have certainly been studying cybersecurity issues now for over a decade, and I have to say, I still learn something every day as the domain and the actors in it continue to evolve.

Secretary Rapuano, it is good to see you once again. We certainly appreciated your testimony on countering weapons of mass destruction a few weeks ago, and I certainly look forward to today's testimony that you will provide on cyber.

And, Admiral Rogers, it is a pleasure to have you back before us again today, and I want to thank you for your service to the Nation. It has been many years that you and I have had the oppor-

tunity to interact, whether it is here on the HASC or in my years on the HPSCI [House Permanent Select Committee on Intelligence], and it has been an honor to work with you. And I am just grateful for everything that you have done and all your contributions to better protecting our Nation's cyberspace. I certainly wish you and your family well as you start the next chapter as well.

2018 is poised to be a notable year for U.S. Cyber Command. Following the legislative action out of this subcommittee over the past several years, CYBERCOM will be elevated to a new unified combatant command [COCOM] after confirmation of the next commander.

Additionally, a cyber posture review is being conducted for the first time, and a legislative framework is in place for notification of sensitive cyber operations. Cyber evaluations of major defense systems continue to be conducted to mitigate known vulnerabilities posing operational or other risk.

Furthermore, cyber activities supporting named and contingency operations overseas have also matured, allowing the Department to leverage lessons learned when it comes to tactics, techniques, and procedures, as well as command and control of our forces.

All teams of the Cyber Mission Force [CMF] are expected to achieve full operational capability [FOC] by the end of the year.

These are all excellent steps forward, toward maintaining our superiority in an ever-changing domain, but, though progress has been made, of course, these efforts and achievements do not mean we have reached the finish line. Instead, I would argue that we have just begun the race.

In addition to reaching FOC, we must ensure that the CMF has the right people, continuous training and education, and the best capabilities in our toolbox to perform against any threats that may confront us. We must be able to measure the readiness of these teams, define the requirements against which they are being or may be employed, and the frameworks in place to rapidly employ them and enable them to respond, when appropriate, based on clear legal policy and operational authorities.

Existing frameworks are too ambiguous to effectively, clearly, concisely, and consistently employ the CMF against all mission sets. Effective and comprehensive policies to deter and respond to adversarial actors, as well as efforts to shape international norms of state behavior, particularly regarding use of military cyber capabilities outside of a combat zone, are progressing more slowly than desired.

As I said at the outset, this domain continues to evolve quickly, and it is simply not good enough to just keep up with our adversaries. Instead, we must set the pace. However, we must not compromise our morals and values when employing cyber forces, for those qualities are what set us apart from those who seek to do us harm.

We must also avoid a cyber cold war of sustained activities carried out by proxies or below the level of armed conflict. Instead, the U.S. must continue leading in crafting of sound domestic and international policies and laws for cyberspace and cyber warfare, working with our allies to assert and enforce rules of the road, rather than letting malicious actors do it for us.

With that, I would like to once again thank our witnesses for being here.

Take care, Admiral Rogers. I thank you again for your service and wish you well.

And, again, thank you for being here today to discuss such an important aspect of our military's capabilities. I strongly believe that each and every conflict we face in the future will contain some element of cyber, and, as such, we must be prepared for all activities in the cyber domain.

With that, I want to thank you all again, and Madam Chair, I yield back.

Ms. STEFANIK. Thank you, Jim.

I would also like to remind members that immediately following this open hearing the subcommittee will reconvene right next door—oh, upstairs for a closed, classified roundtable with our witnesses.

Before we move to our opening statements, I ask unanimous consent that non-subcommittee members be allowed to participate in today's briefing after all subcommittee members have had the opportunity to ask questions. Is there objection?

Without objection, non-subcommittee members will be recognized at the appropriate time for 5 minutes.

Welcome again to our witnesses.

Admiral Rogers, the floor is yours.

STATEMENT OF ADM MICHAEL S. ROGERS, USN, COMMANDER, U.S. CYBER COMMAND, AND DIRECTOR, NATIONAL SECURITY AGENCY

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

On behalf of those hardworking men and women, I am here to discuss the command's posture and describe how we prepare for and execute operations in the cyberspace domain to support the Nation's defense against increasingly sophisticated and capable adversaries.

The cyberspace domain that existed when we first established Cyber Command 8 years ago has evolved dramatically. Today, we face threats that have increased in sophistication, magnitude, intensity, velocity, and volume, threatening our vital national security interests and economic well-being.

Russia and China, which we see as peer or near-peer competitors respectively in cyberspace, remain our greatest concern. But rogue nations like Iran and North Korea have growing capabilities and are using aggressive methods to conduct malicious cyberspace activities. Further, several states have mounted sustained campaigns against our cleared defense contractors to identify and steal key enabling technologies, capabilities, platforms, and systems.

Our adversaries have grown more emboldened, conducting increasingly aggressive activities to extend their influence, with limited fear of consequences. We must change our approaches and responses here if we are to change that dynamic.

While the domain has evolved, Cyber Command's three mission areas endure. Our first priority is the defense of the Department of Defense Information Networks, or DODIN. Second, we support other joint force commanders through the application of offensive cyber capabilities. And, finally, when directed to do so by the President or the Secretary of Defense, we defend critical U.S. infrastructure against a range of significant cyber consequences in support of the Department of Homeland Security [DHS] and others.

In concert with the National Defense Strategy, we are charting a path to achieve and sustain cyberspace superiority to deliver strategic and operational advantage and generate increased options for combatant commanders and policymakers. Without cyberspace superiority on today's battlefield, risk to mission increases across all domains and endangers our security.

Since my last update, Cyber Command has achieved a number of significant milestones.

First, Joint Force Headquarters DODIN, our subordinate headquarters responsible for securing, operating, and defending the Department's complex IT [information technology] infrastructure, has achieved full operational capability.

Secondly, Joint Task Force-Ares [JTF], our warfighting construct focused on the fight against ISIS [Islamic State of Iraq and Syria], has successfully integrated cyberspace operations into the broader military campaign to defeat ISIS. And we will continue to pursue ISIS in support of the Nation's objectives.

Third, we have enhanced our training in cyber operations to prepare the battle space against our key adversaries.

This year will bring several additional accomplishments.

Cyber Command will be elevated to a unified combatant command. As a combatant command, we will have the unique responsibilities of being a joint force provider and a joint force trainer, responsible for providing mission-ready cyberspace operations forces to other combatant commanders and ensuring that joint cyber forces are trained to a high standard and remain interoperable.

In addition, this month, we will start moving in several hundred people into our new, state-of-the-art integrated cyber center and joint operations center at Fort Meade. This will be our first fully integrated operations center that enhances a whole-of-government coordination and improves planning and operations against a range of growing cyber threats.

And within this dynamic domain, it is imperative to continually evolve our training and our tools for our operators. We have recently delivered the first of several foundational toolkits, enabling the Cyber Mission Force to work against adversary networks while reducing risk of exposure, as well as equipping JTF-Ares with capabilities to disrupt ISIS's use of the internet.

Innovation and rapid development demand competition and the ability to leverage all partners, including that of small businesses in the private sector. We intend to create an unclassified collaboration venue where businesses and academia can help tackle tough problems with us without needing to jump through clearance hurdles, which are often very difficult for some of them.

Of course, all of our tools require a talented and sophisticated workforce to operate them. The Cyber Excepted Service, which

Congress has helped create, will help us recruit, manage, and retain cyber expertise in a highly competitive talent market.

Our success also hinges and remains entwined with continued integration of the Reserve and National Guard. In our headquarters, for example, we currently employ more than 300 full-time and part-time reservists. And, in addition, Reserve and National Guard members are mobilized every day to lead and execute cyberspace operations.

Perhaps most significantly, in the coming year, we are nearing completion of the build-out of our Cyber Mission Force, with all of our teams on a glide path to reach full operational capability by the end of fiscal year 2018. And, in fact, we will achieve this goal ahead of time.

And as the teams reach FOC, our focus is on shifting from beyond the build, i.e., creating this force, to ensuring that this force is ready to perform their mission and is optimized to sustain mission outcomes year after year after year.

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

And, as you know, I serve as both Commander of United States Cyber Command and the Director of the National Security Agency. This dual-hat appointment underpins the close partnership between these two organizations. The fiscal year 2017 National Defense Authorization Act [NDAA] includes a provision that describes the conditions for any potential split of this dual-hat arrangement. And the Department is working its way through this question. And, ultimately, the Secretary, in conjunction with the Director of National Intelligence, will provide a recommendation as to the way ahead here to the President.

All of us are proud of the roles we play in our Nation's cyber efforts and are motivated to accomplish our assigned missions, overseen by the Congress, particularly this committee.

And, finally, as you have already mentioned, after serving for over 4 years as the Commander of United States Cyber Command, and after nearly 37 years of service in uniform, I am set to retire later this spring. And, as I do so, I am grateful for the committee and its past and continued support and its confidence in me and in the Cyber Command team.

And I look forward to answering your questions. Thank you very much.

[The prepared statement of Admiral Rogers can be found in the Appendix on page 27.]

Ms. STEFANIK. Thank you.

Assistant Secretary Rapuano.

STATEMENT OF KENNETH P. RAPUANO, ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY, U.S. DEPARTMENT OF DEFENSE

Secretary RAPUANO. Thank you, Chairman Stefanik, Ranking Member Langevin, and members of the committee. It is an honor to appear before you alongside Admiral Rogers, Commander of U.S. Cyber Command, to discuss the Department of Defense's priorities in cyberspace.

In these roles, I oversee the development and implementation of the Department's cyber strategy and policy with regard to cyberspace, leading the Department's interagency cyber coordination efforts, advising the Secretary and the Deputy Secretary on cyberspace activities, and ensuring that the Department's cyber forces and capabilities are integrated across the joint force to support the missions assigned by the President and the Secretary of Defense.

The Department's primary mission is to defend the United States and its interests. My focus from the outset has been on ensuring we are organizing, resourcing, and posturing ourselves to be ready to fight in and through cyberspace in a conflict with great-power competitors.

To that end, we have prioritized the three themes of the 2018 National Defense Strategy: increasing lethality, strengthening alliances, and reforming the Department's practices.

The Department is pushing hard to ensure that we can deter aggression and out-think, out-maneuver, out-partner, and out-innovate our competitors and adversaries in cyberspace.

2018 will be a landmark year when U.S. Cyber Command will elevate to a unified combatant command, welcome a new commander, and complete the force-generation phase of the Cyber Mission Force.

DOD's cyber forces are uniquely responsible for executing both offensive and defensive cyber operations, but national cybersecurity is inherently a team sport. Individuals, corporations, and organizations that own and operate critical networks must take appropriate steps to implement best practices in configuring connected devices and systems to mitigate known vulnerabilities, to harden the most critical networks' systems and information, and to implement basic cyber hygiene and security measurers.

Cybersecurity experts estimate that some 90 percent of cyber attacks could be defeated by better implementation of better cyber hygiene practices and best-practice sharing. Therefore, an essential element of cyber deterrence must be to minimize vulnerabilities that potential adversaries can exploit with significant effects.

Through basic cyber hygiene and information sharing across the government and private sector, we can drastically decrease the opportunities for our adversaries to hold us at risk, and the amount of time and resources we must spend responding to malicious cyber activity directed against us.

We can then devote more capacity to developing and maintaining capabilities to hold our adversaries at risk. The Department is focused on preparations to defend the United States by halting or degrading strategic cyber attacks using cyber effects operations. We also seek to leverage the Department's extensive information collec-

tion mechanisms to provide timely indicators and warnings to public and private owners and operators.

If a cyber attack of significant consequence should occur, the Department of Homeland Security and the Department of Justice, with other departments and agencies in support, would take the lead in responding to, recovering from, and investigating the different elements of a significant cyber incident.

The DOD stands ready to provide additional support to DHS and other Federal agencies upon request. The technical skills possessed by the Cyber Mission Force can augment our interagency partners when the magnitude of a cyber event calls for a collaborative government response. We are currently working with the Department of Homeland Security to determine the most effective and efficient ways for DOD to enhance our support to these efforts.

We must always keep in mind that the capabilities of the Cyber Mission Force were developed and optimized for DOD's warfighting mission. Offensive operations are the means by which the military seizes and retains the initiative while maintaining freedom of action and achieving decisive results.

If and when the Nation faces a large-scale cyber attack, DOD cyber resources will be focused on and most effectively employed in our adversaries' networks—detecting, preventing, preempting, degrading, or defeating malicious cyber activities at their source, as well as holding at risk other critical equities and capabilities of the adversary.

DOD cyber forces must also protect our networks and weapons systems against malicious cyber activity. The Department conducts network defensive operations every day in order to enhance our cyber resiliency. Defending DOD systems also requires identifying and mitigating our own vulnerabilities. We are moving forward to assess and redress major weapons platforms and critical infrastructure vulnerabilities, as mandated by the NDAAs for fiscal years 2016 and 2017.

As outlined in the National Defense Strategy, the Department's weight of effort must be directed toward preparedness for war. At all times we must be ready to respond with both cyber and non-cyber capabilities to malicious cyber activity that results in loss of life, major damage to property, serious adverse foreign policy consequences, or serious economic impact to the United States.

DOD must be prepared to compete and win in conflict below the threshold of conventional war as well. This is commonly referred to as the gray zone.

Our adversaries are adept at calibrating their actions in both the physical and cyber domains so that no single event rises to the level that would merit a significant United States response. However, the cumulative effect of these actions can be significant.

The Department's cyber forces must be prepared to respond to malicious cyber activity in the gray zone by preempting imminent malicious cyber operations, disrupting ongoing malicious cyber activities, supporting other agencies with our technical skills and capacity, and working with and through our allies and partners to apply diplomatic and economic pressure on these actors.

I am grateful for the support we have received from Congress. The hiring authorities you have provided us have been critical to

creating the Cyber Excepted Service. And your generous resourcing of DOD cyber activities has allowed us to stand up the Cyber Mission Force and put U.S. Cyber Command on the path to elevation.

The President's request for FY 2019 helps us sustain that momentum and continue to strengthen DOD's ability to operate in and through cyberspace. The request includes $8.6 billion for cyber-related activities and represents an increase of roughly $600 million over the FY 2018 budget request.

In closing, I would like to thank the subcommittee members for your time and your assistance working alongside us to develop the cyber force the Nation needs. The people in our cyber community are the best in the world, and I am honored to serve with them.

The Department is committed to approaching the development of our cyber capabilities with the sense of urgency warranted by the gravity of threats we face. Our strong relationship with Congress has been a critical component of our success and will remain vital as we continue our work to ensure that the Department's cyber forces are prepared to compete, deter, and win against any opponent.

I look forward to your questions.

[The prepared statement of Secretary Rapuano can be found in the Appendix on page 46.]

Ms. STEFANIK. Thank you for those opening remarks.

I am going to stick to the 5 minutes aggressively to make sure we can get through all of our questions, but I gave you guys some flexibility.

So my first question is: This morning, we heard from former Secretaries Chertoff and Jeh Johnson, as well as General Alexander, former Commander of CYBERCOM, about the importance of continuing to improve interagency collaboration.

And, Assistant Secretary Rapuano, you just referenced in your opening statement how we are currently working with DHS to determine the best way forward, in terms of what DOD's role is.

What steps specifically are being taken by Cyber Command and DOD to build this more integrated, whole-of-government approach? So not broadly that we are working on it, but what are the specific steps?

I will start with you, Assistant Secretary.

Secretary RAPUANO. Thank you.

First, I think it is useful to quickly just review our current activities in terms of working the interagency process.

We chair three of the six Federal centers associated with cyber and cybersecurity. I won't walk through them all, but the Defense Cyber Crime Center; the Cyber Command Joint Ops [Operations] Center, the JOC; and the National Operations Center that is run by NSA. And in all three of those centers, we are engaging with them on a routine basis, all of the key players in the interagency, as well as industry with some of them, to understand both the threats and the areas for collaboration and cooperation.

We are also part of the NCCIC [National Cybersecurity and Communications Integration Center], which the DHS runs at DHS, in terms of coordinating interagency with critical infrastructure and other industry on response to specific cyber threats.

So we have a very solid foundation in terms of relationship and understanding. The issue really is what specific types of capabilities and what thresholds of capacity other agencies would need in different types of circumstances. And then we need to assess that against what our warfighting requirements are and how do we do that balance.

Ms. STEFANIK. Admiral Rogers.

Admiral ROGERS. So, in addition to the individuals integrated from DHS, FBI [Federal Bureau of Investigation], and other partners within my ops structure and my integration in their ops structure, if you will, a series of specific exercises.

We do two major exercises with our DHS and interagency teammates twice a year—I am sorry. It is two exercises occur, two times total for the year. In addition, a series of tabletop exercises. You look at some of the things we have planned in the next 90 days, for example, we are going to be doing some election interaction at a tabletop kind of level with our DHS partners.

The area that I have—you know, I am leaving, as you are aware. The area that I have talked to the team about I really want us to get into next is: Let's get down to the actual center and sector level, because that is where it comes to the day-to-day execution. Guys, if we want to get to speed, we want to get to agility—because, as operational commander, those are big to me. I want to get to speed, and I want to get to agility to actually execute. Let's look at what we can do to actually perhaps integrate at that level.

So that is kind of a future focus for us, as I am moving forward.

Ms. STEFANIK. And I want to build on that. One of the statements this morning was that the lack of a common operating picture impedes our ability to have this comprehensive cyber strategy. What do we do to address this lack of a coherent operating picture?

Admiral ROGERS. For me—I apologize, Ken—first, it is a common operating picture of what? You want an operating picture of critical infrastructure? You want an operating picture of all of private infrastructure?

Ms. STEFANIK. Well, that is part of the question, is——

Admiral ROGERS. Right.

Ms. STEFANIK [continuing]. What is the role of Cyber Command to drive those conversations? What is that interagency process? I think we need to have the answer to all of those.

Admiral ROGERS. So, for me, my input would be, the mission set that I am directly responsible for within the broader DOD effort is the critical infrastructure piece. So I am really interested—so how do we get to an integrated, real-time picture that enables us to have an accurate sense of what is going on that enables decision making and helps to speed that decision making?

So that would be my recommendation for a kind of first focus, even though, as I acknowledge, that is not going to be DOD's lead here. We are in a support team role. But I like to think we need to be part of this discussion and we can help.

Ms. STEFANIK. So how do we spur that, though? I think the status quo is unsustainable. Obviously, we need to spur that interagency integration.

Secretary RAPUANO. I appreciate that you are familiar with the National Cyber Incident Response Framework, but that really does

drive how we organize and operate within the Federal Government in terms of our engagement with industry and other players.

And in the DHS role, in terms of the asset response piece, the FBI has the threat response piece, and then we have the DNI, who has the intelligence integration function.

Ms. STEFANIK. Okay. I am going to have to take the rest for the record.

Mr. Langevin.

[The information referred to can be found in the Appendix on page 67.]

Mr. LANGEVIN. Thank you, Elise.

And I want to again thank our witnesses for being here today.

Secretary Rapuano, as I mentioned in my opening statement, I believe that U.S. policy on title 10 cyber operations needs to be advanced both domestically and internationally in order to effectively employ the force, deter adversarial actors, respond to adversarial cyber actors, and shape international norms for the military use of cyber capabilities.

So what actions are the Department and the administration taking to advance the understanding of and the gaps in existing laws, authorities, and policies relating to cyber operations to develop standard frameworks and guidance?

Secretary RAPUANO. Thank you for the question, Congressman.

As you all appreciate, the challenge associated with defining traditional military activities in the cyber domain is, typically, that is done by looking back historically at what are traditional types of military operations.

In a domain that is so novel in many respects and for which we do not have the empirical data and experience associated with military operations per se, particularly outside zones of conflict, there are some relatively ambiguous areas associated with, well, what constitutes traditional military activities.

This is something that we are looking at within the administration, and we have had a number of discussions with Members and your staffs. So that is an area that we are looking at, in terms of understanding what the trades are and what the implications are of changing the current definition if that were deemed to be warranted.

Mr. LANGEVIN. Okay. That is certainly something the committee is going to continue to provide rigorous oversight on and work with you as we develop.

So how do you intend to "defend forward," in quotes, as is outlined in the new command vision? Do you envision this defensive posture as using CYBERCOM capabilities and intelligence to provide targeted assistance to national assets, including, for example, critical infrastructure? Or would this involve title 10 activities being used to disrupt platforms potentially before an operation actually begins?

Secretary RAPUANO. So, defending forward, in the DOD context, is really looking at the source of the cyber attacks or otherwise malevolent activities. And it is looking at how we can get at it, how we can uproot it, and also how we can hold other equities valued by the adversary perpetrating the act at risk.

And, with that, I will just turn it to Admiral Rogers.

Admiral ROGERS. So the vision you outline is—my goal as a commander is to try to get ahead of problem sets before they occur. Therefore, I am interested in asking myself within the authorities granted to me and within the broad legal framework that we use for the application of DOD capabilities, how can we attempt to forestall activity before it even happens? Failing that, how can we very quickly stop that activity before it has the time or the ability to generate significant impact, if you will, against our critical infrastructure?

And so our strategy is about, how do you tie—or vision is, how do you tie together the power of intelligence and the insights that generates with the operational capability that DOD has invested in the Cyber Command structure in its mission force teams?

And so that is our vision for the future. This capability that we have invested, that we have built, how do we use it in a way that attempts to forestall the opponent's ability to gain advantage in the first place? And, failing that, how do we stop that activity before they are able to have significant impact?

Mr. LANGEVIN. I think it is important to be forward-leaning. I like kind of the shift in focus. And I think the American people, quite frankly, expect that we will be more forward-leaning.

Admiral Rogers and Secretary Rapuano, leveraging the lessons that we have learned to date is important to achieving success in the cyber domain, especially since we are learning as we go. We benefit, obviously, from every success and every failure.

How are our lessons learned from CYBERCOM's mission and operations being leveraged and instituted? And how is readiness being defined for the CMF? And how is this readiness being measured? How are training and recertification processes co-evolving with the threat and the technology landscape?

We will probably run out of time, but I would like that for the record.

Admiral ROGERS. Yes, Sir. So, a lot in that question. Very quickly, it doesn't matter if it is something we do offensively, if it is something we do defensively; every time, part of our mission structure is post-event debrief, analysis, lessons learned, and then how do we tie this into what we are doing next. So there is a cumulative impact there which, as a commander, I really like. You learn——

Ms. STEFANIK. We will have to take the rest for the record.

[The information referred to can be found in the Appendix on page 67.]

Admiral ROGERS. Okay. Got it.

Ms. STEFANIK. We have to move along.

Ms. Cheney.

Ms. CHENEY. Thank you, Madam Chairwoman.

And thanks, Admiral Rogers and Secretary Rapuano.

I am concerned, as is the subcommittee and the entire committee, about the lack of any cyber strategy. We haven't seen anything from the administration, despite the fact that we made requests for it in the NDAA last year.

And I wonder if you could shed some light on why that is, why there is no strategy, number one, and, number two, how we can be in a position, in light of the threats we are facing, in light of the

action that we are seeing, the active measures by our adversaries, to be engaged in any sort of effort to defend or to act offensively without understanding what the overall mission and goals and objectives are in the absence of a strategy.

And I guess I would go to you first, Secretary Rapuano.

Secretary RAPUANO. Thank you.

I think one of the reasons is it is very hard. There are a lot of evolving dynamics at play. And we still have a relatively new administration. And there are competing views as to what the right trade space is associated with a variety of equities and risks.

That said, it is at the White House, the national cyber strategy, and I understand that it should be forthcoming in the near future.

We are looking to then enhance our cyber posture approach, which we will be providing by August, to sync with that national strategy. DOD is one key member of the whole of government, and we want to make sure that we are very thoughtful in terms of very synthesized integration with the national approach.

Admiral ROGERS. And I would only add, I don't think you should feel for 1 minute that that means the DOD, for example, has stood pat and done nothing. We have got a National Security Strategy and a National Defense Strategy in which cyber is a component. As the operational commander, I have tried to take that broad, strategic vision, and, as Representative Langevin has articulated, I have laid out in writing to my team, here is kind of the vision I think that we need to be building to that reflects that broader strategic underpinning, even as I acknowledge we have not yet completed a specific cyber strategy, although that work is, we think, getting close.

So I would only—please don't think that we are just standing still, waiting for someone to tell us, you know, what we——

Ms. CHENEY. No, I appreciate that. I was not under any illusions that you were just standing still, and appreciate very much the work you have done. We want to be helpful, but I think it is also absolutely incumbent upon this administration, in light of this threat, to provide some guidance.

And precisely, Secretary Rapuano, as you said, it is hard, but it is hard because we are in a whole new world, and our adversaries, in fact, are moving forward, and the lack of ability for us, on our part, to say, look, this is what we have to deal with, this is how we are going to operate, this is what we have to guard against.

And, frankly, both in a public and classified setting, being able to say to our adversaries, these are the kinds of things that will result in a response from us, and laying that out so we have a much more effective deterrent policy in place is something that I think we as a subcommittee have got tremendous oversight obligations in looking at it.

And the administration itself—now we have seen significant turnover at the NSC [National Security Council]. I see just news reports now that Nadia Schadlow has resigned. Obviously, Mr. Bossert has moved on. We can't let those add to the amount of time that is going to be dedicated now or taken up in putting the strategy together.

So it is something we will continue to work on in a way so we can ensure that the Nation is, in fact, got a strategy in place to deal with one of the most important and dangerous threats we face.

And I will yield back the balance of my time.

Ms. STEFANIK. Mr. Larsen.

Mr. LARSEN. Thank you, Madam Chair. I will yield my time to Representative Murphy.

Ms. STEFANIK. Mrs. Murphy, you are recognized.

Mrs. MURPHY. Thank you, Admiral Rogers and Mr. Rapuano, for being here.

I am encouraged that the Department is making progress on fielding the Persistent Cyber Training Environment [PCTE], which is, as you know, the training platform that allows cyber forces to train in simulated network environments.

I represent Orlando, which is home to Army's Program Executive Office for Simulation, Training, and Instrumentation, or PEO STRI. PEO STRI was tapped to develop and acquire the PCTE which will also incorporate the work of the National Cyber Range in Orlando.

In your view, what do you think the value of a Persistent Cyber Training Environment is for readiness? What kinds of individual and collective training objectives do you think you can support? And then, as you look into the future, what sorts of capabilities and infrastructure do you foresee these PCTEs requiring?

Admiral ROGERS. So, for me, Cyber Command, we are the ones who articulated the operational requirement, because my vision, our vision, if you will, is I want to be able to, wherever our cyber forces are garrisoned or stationed—we started early on in this process large exercises, brought together literally a thousand individuals, teams from across our force. Those are all good things.

But when I said to myself, look at the time it takes to build this network, the money it costs to do this, while this should be a component of our training strategy, this does not scale for a day-to-day effort. And we need a day-to-day capability that you can train in garrison where, defensively, I can create, I can mirror my own networks, I can simulate an opposing force attempting to penetrate the network, and I can use my defensive techniques to train against it.

Likewise, I can use this, I want to build this over time so I can bring my allies into this so it is not just us, it is our broader international partners, because if it is expensive for us, imagine what it is with some of the work we are doing with nations spread around the world in cyber right now, trying to get them to bring their entire team structure to the United States.

This is also good for me because I want to be able to create network structures that, from an offensive standpoint, I can model. So how am I going to penetrate this? What actions might the defensive team take?

I can use offensive and defensive capability together in head-to-head scenarios where, quite frankly, they are each trying to get the better of the other. Never underestimate the positive impact of competition and a little head-to-head contest to keep teams motivated.

So those are all examples of why I think PCTE is so important for us because that goes to the ability to retain readiness and the ability to be ready now, not, well, if you give me 3 months, if you give me 4 months, whatever. We can't work that way.

Mrs. MURPHY. And you just mentioned the idea of integrating allies and partners into, you know, training together. Where do you think there are some opportunities for enhanced training and security cooperation activities in this space?

And then, do you have some examples of allies and partners where this is already happening that are maybe benchmarks or best practices for how we can move forward?

Admiral ROGERS. So I haven't—most of our international partners, quite frankly, are in the same place we are. They see a need; they see a requirement. They don't yet have in place the long-term solution that they would like.

There's three or four off the top of my head where I have actually sat down with them and said, "Hey, walk me through your system. Can I see what you do?"

We participate in some foreign exercises as well. It isn't just everybody comes to us. I want to learn from others. We participate in foreign cyber exercises.

But I think the ability, particularly for our key—the Five Eyes [1] and a handful of other nations, where we are just part of an ongoing coalition in cyber, if you will, focused on both the defensive side and in some cases the offensive side, the ability to put together an integrated training structure where, again, I can have their units in garrison, we can model the exact terrain that we think we are going to be dealing with live, that is going to be so impactful for our ability to actually execute mission.

Mrs. MURPHY. Yeah. And do you envision that, as you run these exercises and identify vulnerabilities, whether it is in platforms that are ours or allies and partners and their networks, that you will be able to——

Admiral ROGERS. Right, that I would turn them around?

Mrs. MURPHY [continuing]. Turn it around and get it to the——

Admiral ROGERS. Yes, ma'am.

Mrs. MURPHY [continuing]. Folks who are building that so that they can address them?

Admiral ROGERS. Yep. That is part of the idea here.

Mrs. MURPHY. Great.

And then you have stated in your testimony that CYBERCOM is working to synchronize cyber planning and operations across the entire joint force and that CYBERCOM is helping the combatant commands improve command and control by establishing integrated planning elements——

Admiral ROGERS. Right.

Mrs. MURPHY [continuing]. At each COCOM.

Can you provide a little more detail on exactly how CYBERCOM is standing up—is it CO–IPEs [Cyber Operations–Integrated Planning Elements]?

Admiral ROGERS. CO–IPEs, yes, ma'am.

---

[1] An intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States.

Mrs. MURPHY [continuing]. At each COCOM?

Admiral ROGERS. So there's nine other COCOMs besides us. We become the 10th one effective with the new commander being confirmed and assuming the duties.

I thought one of the biggest shortfalls we had was—I thought we did a great job with the Cyber Mission Force in creating a higher headquarters in the form of Cyber Command. But if you truly want to integrate cyber into the breadth of operations across this Department, then you have to integrate this capability at all the COCOMs. And so we——

Ms. STEFANIK. Admiral Rogers, we will have to take the rest for the record. It was a good question.

[The information referred to can be found in the Appendix on page 68.]

Mrs. MURPHY. Thank you.

Ms. STEFANIK. Mr. Scott.

Mr. SCOTT. Thank you, Madam Chair.

Admiral, you mentioned authorities a little earlier. What would CYBERCOM require to move from a defensive support posture to an active deterrence posture, where you were actually hunting and denying malicious operators before they inflicted damage?

Admiral ROGERS. So, for right now, if you look at day-to-day authority that is currently granted to the commander of Cyber Command, on the defensive side, I feel very good that I have the authorities that I need to defend the DODIN, the DOD networks.

But one of the questions I think we need to ask ourselves is, for example, with the defense industrial base, or if DOD's role is going to be to partner in defending critical infrastructure, what level of ability to operate outside the DODIN would be appropriate for the Cyber Mission Force. I think that is a good conversation for us to have. Because, right now—again, not a criticism; an observation. Right now, you know, the current construct, I don't operate outside the DODIN. So I would suggest we ought to take a look at that.

On the offensive side, I very feel very comfortable about the authorities that we have currently put in place to apply cyber in areas of designated hostility—the Syrias, the Iraqs, the Afghanistans of the world. And we are doing operations there almost every day.

The area where I think we still need to get to a little more speed and agility—and, as Mr. Rapuano has indicated, it is an area that is currently under review right now; we are working our way through—is what is the level of comfort in applying those capabilities outside of designated areas of hostility and how could we potentially speed that up.

I don't believe that anybody should grant Cyber Command or Admiral Rogers a blank ticket to do whatever they want. That is not appropriate. The part I am trying to figure out is what is an appropriate balance to ensure that the broader set of stakeholders here have a voice in what we do but, at the same time, we empower our capabilities with speed and agility to actually have meaningful impact. And I think that is what we are trying to work our way through right now.

Mr. SCOTT. And so that brings me to the next question, which deals with the Guard as they establish cyber units. I know you said

you had 300 full- and part-time working with you right now at U.S. CYBERCOM. These units, I mean, they will not only be supportive of their home States, but I assume that we would want them to have the authority to be supportive of other States as well.

Admiral ROGERS. A lot of it depends—so, first of all, I am the son of a Guardsman, so I grew up—my father was in the Illinois Guard for 27 years, so, as a kid—you know, so I feel very strongly about the value of the Guard. I have lived this personally, and I saw the difference my father made when he served.

The challenge, I think, is: How do we view this as an integrated whole? So one of the points I make to the Guard and I make to the Governors when they ask me this question: Remember, we are all competing for the same manpower pool, if you will. There are only so many people out there with the requisite skills and kind of background. So be leery of doing solution sets where we try to replicate, for example, 50 different independent capabilities across every single State. It is, how do we synchronize this?

The other point I try to make is: Remember, cyber doesn't recognize geography. So I am a resident of the State of Illinois. And if you are trying to protect infrastructure in Illinois, the challenge might be that much of that infrastructure physically doesn't even reside in Illinois. It is the way that the digital backbone has been built.

So title 32 and the Guard's employment outside of title 10 is all based on legal authority that also has a key geography component. You are acting in a title 32 capacity within your State. What do we do when the cyber infrastructure that you are trying to defend or impact doesn't reside in that physical location?

So my only argument is: We need to work our way through this, and we need to think more broadly and in a more integrated approach. So I don't think it is only Guard and Reserve. Likewise, I don't think it is only Active. We have to get across the spectrum. And we have to ask ourselves, whatever we create, how do we do it in a way that maximizes its ability to be employed in potentially multiple different scenarios, not just a scenario, if that makes sense.

Mr. SCOTT. Absolutely. It is complex.

And the city of Atlanta, as you know, was subject to a ransomware attack. And, you know, I can see that—I mean, I think the SamSam ransomware has been around for 8 years now. I mean, I can see this as we talk about infrastructure; it is not just going to be attacks on DOD and on U.S. Government operations. It is going to be attacking State operations and city operations.

And I, quite honestly, don't care where the person comes from that stops the attack, nor do I think any other government official would. And just, we will need help with how we draft that language for you.

And, with that, I yield the remainder of my time.

Ms. STEFANIK. Mrs. Murphy.

Mrs. MURPHY. Thank you, Madam Chair.

I just wanted to use the rest of my time to let you finish that question. Because you were talking about, you know, that it needs to be integrated into the COCOMs.

Admiral ROGERS. Right.

Mrs. MURPHY. But, as you finish that, also, if you can talk to me a little bit about how J5 will integrate with these CO–IPEs and whether or not you have both the manpower and the capacity to and a solid handle on the CYBERCOM plans in order to make sure that they are synchronized.

Admiral ROGERS. Right.

So one component was we have to get knowledge and experience at the COCOM level on how you plan and execute cyber operations.

Secondly, that capability has to be able to be integrated not just within that particular COCOM—Honolulu, Stuttgart, Tampa, fill in the blank—but it has also got to tie back to Cyber Command so that we have one integrated approach to how we are doing business here, particularly since the majority, all of the offensive capability within the Department, for example, remains under my, Cyber Command's operational control. We apply it in support of the other combatant commanders. So we have got to tie this together.

We are starting the build in 2018. It is going be finished by 2023, so it is a 5-year build-out. We will have IOC [initial operational capability] at all nine projected by the end of 2019, so by the end of the next fiscal year. That gets an initial operating capability to all of the other nine combatant commanders. And then we will flesh it out over the course of the next 3 years.

A couple of COCOMs are a little further than others, and we are using as kind of a test case then. I would highlight—and no disrespect to any, but I would highlight PACOM [U.S. Pacific Command] and CENTCOM [U.S. Central Command], probably the two where, at the moment, we have started to get the initial investments, and because of some of the broader activity in their theaters that are of high interest, that are bringing our cyber capability to bear, along with a lot of other capabilities, we have kind of decided to use them as a bit of a test case, if you will.

Mrs. MURPHY. Uh-huh. Great.

And, I guess, are you going to be also providing the training and resources to help people have the cyber fluency to be able to engage even if that is not their primary mission?

Admiral ROGERS. Right. So part of this is we will help develop the training standards for every one of the billets.

This is also a good example of how, once—with each service having created a core cyber competency, one of my visions is, so you could do one tour at a combatant commander, you could do another tour in one of our mission teams, you could do another tour at Cyber Command, you could do another tour in ASD [Assistant Secretary of Defense] in Cyber Policy, you could go to the Joint Staff and do cyber work.

Mrs. MURPHY. Uh-huh.

Admiral ROGERS. One of the values of this professionalization that, as a Department, we have put in place now is that we will get recurring benefit by moving people so we don't have to train every—so it is the first time you have ever done this; we don't want to go through that every time. There is always a first time, but I don't want to have to do that every time, if I can avoid it.

Mrs. MURPHY. Great. Thank you very much.

And I yield back.

Ms. STEFANIK. Mr. Garamendi.

Mr. GARAMENDI. I will pass.

Ms. STEFANIK. That concludes the open portion of this session. We are now going to move to 2337.

I also want to just let the members know we are going to have a quarterly cyber briefing. So if there are questions you have that we didn't get to today, that will be scheduled in the coming weeks.

So, with that, this is gaveled out, and we will hustle upstairs.

[Whereupon, at 4:23 p.m., the subcommittee proceeded in closed session.]

A P P E N D I X

APRIL 11, 2018

PREPARED STATEMENTS SUBMITTED FOR THE RECORD

APRIL 11, 2018

Opening Statement
Chairwoman Elise M. Stefanik
Emerging Threats and Capabilities Subcommittee

A Review and Assessment of the Department of Defense Budget, Strategy, Policy, and Programs for Cyber Operations and U.S. Cyber Command for Fiscal Year 2019

April 11, 2018

The subcommittee will come to order.

Welcome everyone to today's hearing of the Emerging Threats and Capabilities Subcommittee on the posture of Cyber Operations and U.S. Cyber Command for Fiscal Year 2019.

This hearing is the second of three cyber events today. This morning we heard from former Secretaries of Homeland Security Chertoff and Johnson, as well as former CYBERCOM Commander Keith Alexander.

Adversaries such as China and Russia aggressively leverage and integrate cyber, information, and communications technologies for geopolitical and economic gain; and they do so in a seamless way. Dictatorships have those advantages, and their control over these technologies and information is as much about exerting control over their own populations, as it is confronting free societies such as ours.

As discussed in the World Wide Threat Assessment for 2018 from the Director of National Intelligence, Iran and North Korea also continue to increase their offensive cyber capabilities and techniques. Over the last few years, both of these nations are believed to be behind cyber attacks that demonstrate not only a capability to deploy a variety of techniques and tools, but also a willingness to use cyber attacks as a means to achieve their national objectives.

Needless to say, cyber threats today from state and non-state adversaries are real, pervasive, and growing. Cyberspace and the information domain writ large remains contested and under continual stress.

We are no longer peerless, and cyber superiority is not assured.

Yet while these adversaries continue to use cyber as a means to achieve strategic objectives, I remain concerned that we – as a government – do not yet have a strategy in place to mitigate, deter or oppose their advances.

It is safe to say that we have improved our **military** cyberspace and cyber warfare capabilities, and also improved our resiliency in many areas.

But I am not sure the same can be said about the rest of our government, most notably the protection of our critical infrastructure that preserves our economic security and ensures our way of life. Further work is needed to build interagency partnerships to ensure a whole of government approach to countering the growing cyber threat.

The Department of Defense plays an important role in this area – certainly when considering a significant cyber incident that may require their expertise during a time sensitive emergency.

From where I stand, a great deal of work remains to be done, to improve our ability to defend, fight, and win in this critical domain.

And also, to improve and align our decision-making processes and operational authorities so that we are fast, agile, and relevant.

Only then will our Nation be prepared for the 21st century challenges we face.

Our witnesses today are very well qualified to help us navigate these multidimensional problems.

Appearing before our subcommittee we have:

Admiral Mike Rogers,
Commander of U.S. Cyber Command and
Director of the National Security Agency

And

The Honorable Kenneth Rapuano
Assistant Secretary of Defense for Homeland Defense and Global Security
and Principal Cyber Advisor for the Secretary of Defense

Thank you both for being here today.

Admiral Rogers – as this will be your last appearance before the subcommittee I would like to extend my sincere thanks and appreciation for your decades of service to our country. We wish you continued success as you move into this next phase of your career and life out of uniform. Thank you for your service and the professional working relationship you have always had with this committee.

I would like to remind members that immediately following this open hearing, the subcommittee will reconvene upstairs for a closed, classified Roundtable with our witnesses.

Welcome again to both of our witnesses. Admiral Rogers, we will begin with you.

STATEMENT OF
ADMIRAL MICHAEL S. ROGERS
COMMANDER
UNITED STATES CYBER COMMAND
BEFORE THE
HOUSE COMMITTEE ON ARMED SERVICES
EMERGING THREATS AND CAPABILITIES SUBCOMMITTEE
11 APRIL 2018

Chairman Stefanik, Ranking Member Langevin, and distinguished members of the Subcommittee, thank you very much for inviting me before you today to represent the men and women of U.S. Cyber Command (USCYBERCOM). I am honored to lead this fine group of Americans, and to speak in public about their accomplishments – which we owe in no small part to the support of the Congress and of this committee in particular. I am also pleased to appear today beside the Hon. Kenneth P. Rapuano, Assistant Secretary of Defense for Homeland Defense and Global Security, who has provided vital support for USCYBERCOM. I expect this will be my last time speaking to you about USCYBERCOM, which is on the verge of becoming a full, unified combatant command, and so I am eager to begin and to answer any questions or address any concerns that you might have. I look forward to a dialogue with you about what we are seeing in cyberspace and what that means for our command, for the Department of Defense, and for our nation.

U.S. Cyber Command's mission is to direct, synchronize, and coordinate cyberspace planning and operations to defend and advance national interests in collaboration with domestic and international partners. We have three mission objectives: to ensure DoD mission assurance by directing the operation and defense of the Department of Defense's information networks (what we call the DoDIN); to deter or defeat strategic threats to U.S. interests and infrastructure; and to achieve Joint Force commander objectives in and through cyberspace. The Command is based at Fort Meade, Maryland, and in this fiscal year is executing more than $600 million dollars in programs and projects. Our full-time staff amounts to 1,060 military members and civilians, plus contractors. At the end of December, we had 5,070 service members and civilians in our Cyber Mission Force (CMF), building to a total of 6,187 people, meaning the CMF was staffed at 82 percent.

Our team is organized into components that together represent all the Armed Services. Officers and enlisted personnel come from each one of the Armed Services, and are organized, trained, and equipped by our Service cyber components in Army Cyber Command, Marine Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, and Air Forces Cyber/24th Air Force (as well as U.S. Coast Guard Cyber). USCYBERCOM proper comprises a headquarters organization and runs operations through its components: the Cyber National

Mission Force (CNMF), Joint Force Headquarters-DoDIN, plus four other Joint Force headquarters elements, each of which is paired with one of the four Services' cyber components named above. Both Active Duty and Reserve Component personnel serve in our forces, and they are joined by Coast Guardsmen as well.

USCYBERCOM performs its missions in accordance with national and department-wide strategic guidance. In elevating USCYBERCOM to unified combatant command status, the President and the Secretary of Defense made several stipulations about its mission and duties, and I shall say more about those in a moment. I hope to impart to you today my sense of the unique value that our Command, acting within these parameters, adds to the defense of the United States and its interests. First I want to give you a sense of the operating environment before us and the gravity of several current and looming cyber threats.

The Cyberspace Environment

We face a growing variety of threats from adversaries acting with precision and boldness, and often with stealth. U.S. Cyber Command engages with adversaries in cyberspace every day. Accordingly, we have developed substantial knowledge of how malicious cyber actors work against the United States, our allies and partners, and many other targets as well. That knowledge in turn provides insights into the motivations, capabilities, and intentions of those who sponsor such activities, whether they be states, criminal enterprises, or violent extremists. Cyberspace is a global and dynamic operating environment, with unique challenges.

A significant story in cyberspace over the past year relates to the progress made against the Islamic State in Iraq and Syria (ISIS), and USCYBERCOM contributions to the eviction of ISIS fighters from their geographic strongholds. Today, ISIS's so-called "Caliphate" is crumbling. It has lost 98 percent of the territory it once controlled in Iraq and Syria, and approximately 3.2 million Syrians and 4.5 million Iraqis now have a pathway to begin to rebuild their cities and their lives. Denying sanctuary to ISIS in Iraq and Syria is a victory for civilization, and an important step in stabilizing the nations of that region and building peace in the Middle East. Cyberspace operations played an important role in this campaign, with

USCYBERCOM supporting the successful offensive by U.S. Central Command (USCENTCOM), U.S. Special Operations Command (USSOCOM), and our coalition partners. We learned a great deal performing those missions, and continue to execute some today. Mounting cyber operations against ISIS helped us re-learn and reinforce important lessons learned over the last decade of cyber operations against violent extremists. I should emphasize that this campaign was a coalition fight, with key international partners conducting and supporting both kinetic and cyberspace operations against ISIS.

The near defeat of ISIS in its geographic strongholds is bringing to a close one chapter in an enduring campaign against violent extremists, but is not the end of the story. While ISIS has lost much of its geographic base in Iraq and Syria, we believe its leaders and die-hard adherents planned for this development. To be clear, the reduction of kinetic combat operations does not mean we have achieved the enduring defeat of ISIS. Without continued attention and support, we risk the return of violent extremist groups like ISIS in liberated areas in Iraq and Syria and their spread in new locations. As the Coalition has made progress in Iraq and Syria, many ISIS fighters, including thousands and potentially tens of thousands of foreign fighters, have fled the battlefield in Iraq and Syria. These members have dispersed to locations around the globe including Africa, Europe, Asia, and other nations in the Middle East, in many cases to reinforce other ISIS branches and affiliates. Carrying their poisonous ideology and experiences with them, they are assimilating into local populations, developing new local and online networks, and overwhelming law enforcement's ability to monitor all of these potential threats our partners' homelands, and potentially our own.

Over the last few years, ISIS fighters and sympathizers have complicated the picture in Afghanistan, frustrating the central government's efforts to bring order and development to that war-torn land. We have watched and opposed their emergence on the battlefield and in cyberspace, and noted their conflicts with the government in Kabul and other insurgent groups. The Afghan area of hostilities represents another important operating area for cyberspace operations. USCYBERCOM is in the fight there as well, employing cyberspace operations to protect coalition forces, target terrorist leaders, and disrupt the operations of hostile forces. We

are providing similar support to our forces battling other violent extremist groups in Africa and Asia.

We believe we may also face a further evolution of the cyberspace threat from violent extremist elements. Since its inception, ISIS leaders and their technical experts have maintained a robust online presence, and we assess that they will seek to increase their efforts in and through cyberspace. They and other groups, such as al Qaeda and its affiliates, still use the Internet to market their versions of terrorism, garner financial and material support, and inspire followers. ISIS, like al Qaeda before it, has worked hard to target susceptible individuals and inspire them to commit attacks in the West. That is why USCYBERCOM works with law enforcement, intelligence, and liaison partners to find and destroy the key nodes in ISIS online infrastructure and media operations (along with the analogous infrastructures of other violent extremists).

Our greatest concern, of course, remains that of actions by state-sponsored malicious cyber actors and the states behind them. We find that many states now seek to integrate cyberspace operations with the plans and capabilities of their traditional military capabilities. Indeed, several have mounted sustained campaigns to scout and access our key enabling technologies, capabilities, platforms and systems as cleared defense contractors develop and produce them. As the Secretary's new *National Defense Strategy* emphasizes, the states of greatest concern are Russia and China, with their advanced technological bases, powerful conventional forces, and nuclear arsenals. We watch them not just because they are big and well-armed, but because they practice coercive diplomacy against their neighbors, and their strategic intentions remain unclear. These two nations also count as peer or near-peer competitors in cyberspace.

China has shown a worrying tendency to challenge the existing rules-based order, from which it has been a major beneficiary. It is pursuing its economic and diplomatic interests with greater assertiveness, rejecting, ignoring, or trying to rewrite norms that it perceives do not trend in its favor. China's behavior in cyberspace exemplifies this trend. For example, Presidents Obama and Xi committed in 2015 that our two countries would not conduct or knowingly support cyber-enabled theft of intellectual property for commercial gain. Subsequent evidence,

however, suggests that hackers based in China sustained cyber espionage that exploited the business secrets and intellectual property of American businesses, universities, and defense industries. The Justice Department just last fall unsealed indictments against three Chinese nationals, alleging they exfiltrated more than 400GB of data from several companies in the United States. In addition, the Chinese government could exploit the production of information and technology products to harvest corporate, government, and even personal data from foreign countries.

Russia represents a different sort of problem in cyberspace. The Intelligence Community concluded last year that Russian actors, with the knowledge of senior decision-makers, employed influence operations to interfere with the U.S. presidential election in 2016. In recent months, Congress has heard testimony from leading social-media companies explaining that their business records had logged an even wider pattern of Russian cyber meddling before the election -- one that matched malicious cyber activities seen by several other nations. The Kremlin has used hackers to steal personal communications that Russian operatives then parceled out in targeted leaks, and created fake social media personas and news items on all sides of controversial issues in the hope of stirring discord in the West. The idea is to make Western electorates distrust all news outlets and ultimately one another. This threatens the foundations of democracy, making it difficult to discern Moscow's intentions and to craft common measures for countering Russia's aggressive actions in its near-abroad and its repression at home.

Russian-sponsored malicious cyber activities of concern to the United States and its allies extend well beyond the behavior cited above. Russian intelligence agencies run their own cyber theft campaigns – witness last November's plea bargain of a foreign hacker who admitted to working on behalf of one of Moscow's intelligence services, wherein he hacked the webmail accounts of individuals of interest to Russia and sold their passwords to his Russian handlers.

We are monitoring the cyber conflict sparked by the ongoing Russian-manufactured conflict in Ukraine. Secretary Mattis in Kyiv noted that Russia is not adhering to the letter or the spirit of its treaty commitments, most egregiously by attempting to change international borders by force. This behavior in geographic space matches Russian cyberspace behavior; Russia's

cyber actions seem designed to complement and support its aggressive actions on the ground. While we cannot discuss the details in open session, I would draw your attention to the spate of very serious cyber attacks against Ukrainian citizens and infrastructure over the last 16 months. For instance, the National Cybersecurity and Communications Integration Center (NCCIC) of the Department of Homeland Security issued an alert in July to public utilities concerning a new malware that targeted electrical grids in Ukraine the previous winter. Last June, the Russian military launched the most costly cyber-attack in history, NotPetya. NotPetya encrypted and essentially ruined hard drives on thousands of Ukrainian computers. This cyber attack quickly spread well beyond Ukraine, causing billions of dollars in damages to businesses across Europe and as far away as the United States.

Most states lack the suite of diplomatic, military, and economic tools employed by Russia and China, but rogue regimes nonetheless cause concern because of their aggressive unpredictability in cyberspace. Iran and North Korea have growing capabilities in cyberspace, and although they have fewer technical tools, they employ aggressive methods to carry out malicious cyberspace activities. The Iranians recruit hackers for cyberespionage, surveillance of their population, cyber attacks on their neighbors and perceived opponents, and even attempts to penetrate our military systems. North Korea has limited Internet-internet connectivity and likely views the Internet as a vector to employ in striking opponents and deterring potential threats. Pyongyang also uses cyber tools to evade economic sanctions and harvest hard currency for Kim Jong-Un's impoverished regime. The United States and our British allies have publicly attributed to North Korea last summer's WannaCry ransomware attacks; 51.92 in bitcoin, worth approximately $140,000 at that time, was transferred out of the bitcoin wallet used by WannaCry—one of many ways of using cyber techniques to generate revenue. Most concerning, we do not see these actors having the technical competence or imperative to avoid uncontrolled damage if they conduct cyber attacks against private-sector targets, especially critical infrastructure.

Various non-state actors in cyberspace cause us concern as well. The main operational problem is distinguishing their efforts and activities from the state-sponsored campaigns. Cyber

criminals and terrorists increase the "noise level" for systems administrators and network defenders everywhere.

In this context, I should mention that improved attribution is in our strategic interest, but not strictly necessary to guard against many cyber threats. A particular malware is still dangerous whether it was developed and/or employed by organized criminals, ideological hactivists, or a state entity. The last year has witnessed an alarming spate of incidents involving increasingly sophisticated cyber tools. NotPetya and WannaCry, for example, both modified powerful tools posted on-line by an anonymous group calling itself Shadow Brokers. What makes this trend even more worrisome is the uncontrolled use of these destructive cyber tools, the wielders of which clearly did not care whether they disrupted or damaged systems far beyond their main targets. We have reason to believe that particular states are behind some of these cyber attacks, and the fact that they have cavalierly unleashed tools that damaged the computers of their own citizens, speaks volumes about their disregard for responsible state behavior in cyberspace. DoD systems escaped particular harm in these incidents, but that is because we made robust and early investments in active, layered defenses. Not everyone has such resources, and so innocent victims had their hard drives encrypted, their data stolen, and their businesses damaged. We do not have to gain positive attribution to each particular actor before we can act to protect ourselves and our allies and partners; in fact, all users must take basic steps to secure their data and systems. We need decisive responses at scale to threats and intrusions. That is where USCYBERCOM finds its mission.

Three Milestones

Several developments will make 2018 a pivotal year for USCYBERCOM.

The first is USCYBERCOM's elevation to unified-combatant-command status. This will take place upon the confirmation and appointment of my successor, who the President recently nominated. The elevation of USCYBERCOM demonstrates to international partners and adversaries our stake in cyberspace, and shows that DoD is prioritizing efforts to build cyber defense and resilience. Elevation reflects the importance of growing threats in cyberspace, and

demonstrates that the United States is maintaining a leadership role. My successor will naturally want to make adjustments at USCYBERCOM to reflect his vision, but in many ways elevation will not drive sudden changes in primary aspects of the Command. The Commander of USCYBERCOM will remain dual-hatted as the Director of the National Security Agency/Chief, Central Security Service (NSA/CSS) in the near term. We at USCYBERCOM are already operating in the cyber mission space and have key partners among U.S. government agencies and allies. These will remain constants for the foreseeable future.

In the long term, elevation entails significant adjustments in USCYBERCOM. You can grasp the implications by consulting the new Unified Command Plan (UCP) that the President approved in November 2017. The UCP made USCYBERCOM responsible for the planning and execution of global cyberspace operations. The responsibilities assigned to USCYBERCOM include: directing the operations, security, and defense of the DoDIN; directing cyber defenses of the critical infrastructure that assures the Department can accomplish its missions; warning and defending against significant cyber attacks on the United States and its interests; coordinating across the Department and the U.S. Government before mounting operations that include our own cyber attack actions; detailing military liaison officers to U.S. Government and international agencies to represent the Command on cyber matters; advocating for cyberspace capabilities in the Department's programming and budgeting processes; integrating theater security cooperation of cyberspace operations in support of Joint Force commanders; and executing cyberspace operations in support of military and civilian authorities defending the homeland, as directed.

The Unified Command Plan also gave USCYBERCOM new duties in keeping with Congress's intent to make it something of a hybrid command along the general lines of U.S. Special Operations Command. Under its new Joint Force Provider responsibilities, as specified in the UCP, USCYBERCOM provides "mission-ready Cyber Mission Forces" to support Combatant Command mission requirements and identifies for the Chairman of the Joint Chiefs of Staff relevant "global joint sourcing solutions" (and supervises their implementation). In addition, under its new Joint Force Trainer role, USCYBERCOM ensures that joint cyber forces are trained and interoperable; sets standards for all joint cyber forces; conducts and supports

combatant command-level exercises; and recommends strategy, doctrine, and procedures for joint cyberspace operations. With our new, Service-like functions, we will be: preparing and submitting program recommendations and budget proposals for cyber operations forces; validating and prioritizing requirements, to include capabilities in any domain that enable employment of cyberspace capabilities; diversifying operational infrastructure; formulating and submitting requirements for intelligence support; coordinating with Military Departments on promotion, assignment, and recruitment of cyberspace operations forces; and exercising limited acquisition authority consistent with Section 923 of the FY17 National Defense Authorization Act (NDAA) and Section 807 of the FY16 NDAA.

One would be correct in inferring from this list of responsibilities that USCYBERCOM must make significant changes over the next couple years while executing its expanding mission. Many of our leaders, teams, and action officers will thus be working double duty, directing and supporting ongoing cyberspace operations while overseeing the changes required by elevation as directed in the UCP. I need hardly add that the stability and hence predictability of our resource flow is especially important during this time.

The second important development to report is the progress of the Cyber Mission Force, specifically our projected completion of the force generation of the 133 CMF teams, with all of them attaining full operational capability by September. In fact, we might meet this target even earlier, likely in June of this year. This long-anticipated milestone is due to the years of hard work by the Services and the agencies, with the support of Congress. We at USCYBERCOM are completing the readiness management programs that will sustain the readiness of the CMF teams. After all, commissioning a warship – while an important event – does not make that ship mission-ready. On a ship, as on a Cyber Mission Force team, much work remains to be done to make the crew members proficient at their duties and the whole team ready and able to perform whatever missions might be directed.

Finally, in a matter of weeks USCYBERCOM will open its new Integrated Cyber Center and Joint Operations Center (ICC/JOC) at Fort Meade. Construction is nearly complete, and we will begin moving forces into the building in April. The facility is USCYBERCOM's first

dedicated building, providing the advanced command and control capabilities and global integration capabilities that we require to perform our missions. I am grateful for the congressional support that brought us so far in this long process, and of course I invite members of the Committee to visit Fort Meade for a tour of our new facility.

On a related note, later this year USCYBERCOM will formally request your support for a new headquarters facility. My headquarters operates today from dozens of office suites in ten NSA-owned or -leased buildings dispersed across 50 square miles of the Baltimore-Washington Highway corridor. No other Combatant Commander confronts such an obstacle, which makes efficient and effective staff function challenging. In an operating environment where seconds matter, we require a headquarters that facilitates staff and partner integration, information flow, and rapid decision-making. I believe the right location for our headquarters is on Fort Meade in a purpose-built facility, and I will request your support for this requirement.

US Cyber Command's Missions and Performance

Our first and primary mission objective remains defending the information systems of the Department of Defense. Adversaries realized decades ago that the power of the U.S. military in no small part derives from its integrated and synchronized functioning, which in turn relies on networks, bandwidth, processing, and analytics. Operations, sustainment, intelligence, and command and control rely on sensitive networks linked across the public Internet infrastructure. Attacking our information systems looks to some adversaries like a way to stop the U.S. military. We know this because we read their doctrinal writings, we watch their probes of our systems, and we see how they monitor our personnel. If their efforts to penetrate the DoDIN were to succeed and open avenues for attacks on our DoD networks and systems, then my fellow Joint Force commanders would find it difficult to execute their respective missions.

Securing and defending the DoDIN is a crucial, 24-hour-a-day task. The old adage remains true: an ounce of prevention is worth a pound of cure. Secure information systems free us from the expense and time of remedying preventable intrusions, breaches, and disruptions. The WannaCry and NotPetya malwares mentioned above, for instance, exploited a vulnerability

in Windows that Microsoft Corporation had patched weeks earlier. Many enterprises and users had installed those patches as a matter of course, keeping current with their security updates – as we had on the DoDIN. We and they thus remained largely unharmed by these two outbreaks. And no sooner did 2018 begin, than new challenges presented themselves in the form of widespread vulnerabilities -- dubbed Meltdown and Spectre – that are inherent in nearly all computer processors. Coordinating such preventive measures in a timely fashion and across a huge enterprise like the DoDIN is no easy feat, yet we have learned to do so in a regular, timely, and accountable manner. That is not to say that we do everything right in operating the DoDIN; it is rather to reiterate the importance of a central command authority to assess operational risks, direct responses, and hold administrators accountable for executing prescribed remedies.

We see evidence every day that adversaries continue to probe the DoDIN. Most probes represent attempted espionage rather than cyber attacks, but cumulatively they force us to devote considerable resources and attention to defense – which perhaps is the intention behind them. Over the past year, our Cyber Protection Teams were fully engaged with testing our systems and supporting the defensive efforts of our mission partners (more on this below). We appreciate the intent of Congress to assist us in this field as voiced in Section 1640 of the FY18 NDAA. That measure requires the Department of Defense to outline a Strategic Cybersecurity Program to work with USCYBERCOM in reviewing the cybersecurity of critical defense capabilities like nuclear command and control, sensitive information systems, and long-range strike assets.

Keeping DoD's information networks, weapons systems, and affiliated networks functioning and secure requires teamwork by many partners, particularly the Services, NSA, the Defense Information Systems Agency (DISA), the DoD Chief Information Officer (CIO), and the various cybersecurity service providers (CSSPs). In our experience, successfully defending our systems requires the application of time-tested operational principles for the Joint Force, as well as a tight connection with the activities to secure all DoD networked devices. In this regard, I am naturally concerned with any legislative or policy proposals that would take the management of operational risks out of the military chain of command and vest it in civilian staff or advisory components of DoD. I would point you specifically to language passed in the FY18 NDAA (Sec. 909) that provisionally authorizes the DoD CIO to set standards for and certify

capabilities on DoD networks. This provision could be interpreted to make an official outside the military chain of command responsible for determining which capabilities a Joint Force commander can employ to perform his missions, and interpose another layer of review and delay in a development and acquisition process that greatly needs speed and agility.

To explain my reasoning here, the DoDIN is equivalent to a joint security area in the terrain of cyberspace—essentially a set of bases and communications assets that enable and facilitate operations and mission accomplishment by the entire Joint Force. I am responsible for the security, operation, and defense of this joint security area, and my ability to accomplish that mission is affected daily by the ever-shifting dynamics on the physical, logical, and persona levels that together constitute its terrain. I must both protect this terrain against potential threats and defend it against specific threat actors. The design, fielding, and operation of DoD information technology directly affects how I can move and maneuver to defend the DoDIN, and thus the degree of risk that I must assume (and indirectly the degree of risk imposed on the entire Joint Force). As the commander, I should be the decision-maker for accepting and managing operational risks on the DoDIN. It would also help for me to have a significant degree of influence in the development, adaptation, policy, and standards of DoD information technology, networks, and cyberspace capabilities.

Our second major mission objective is to defend the United States against cyber threats to U.S. interests and infrastructure. We are concerned that many such cyber attacks now occur below the threshold of the use of force and outside of the context of armed conflict, but cumulatively accrue strategic gains to our adversaries. The United States must continuously and persistently engage and contest cyber attacks, in order to reset adversary expectations about our behavior and commitment. The Secretary's new *National Defense Strategy* speaks to this point in discussing the Global Operating Model for the Joint Force, in which cyber is a foundational capability that remains in contact with adversaries "to help us compete more effectively below the level of armed conflict." Through consistent action, and in coordination with interagency partners, we can influence the calculus of hostile actors, deter malicious cyber activities, and clarify the distinction between acceptable and unacceptable behavior in cyberspace. Cyber capabilities can also disrupt and potentially deter non-cyber threats as well.

The importance of cyberspace for our nation's security and prosperity demands unified responses across departments and agencies regardless of sector or geography. Cyber capabilities should be integrated with plans and operations across all domains to influence and shape adversary behavior, in preparation for and during joint operations in a conflict, as well as outside of situations of armed conflict.

Equally integral to defending the nation against cyber attacks is collective defense and collaboration with our allies and partners, both domestically and abroad. USCYBERCOM facilitates whole-of-government planning. We are helping DoD increase collective situational awareness through our collaboration with partners like the Department of Homeland Security (DHS), the FBI, the Department of State, and other departments and agencies. Working with our interagency partners, we have also matured our collaboration with key critical infrastructure sectors. Such collaboration allows us to better understand events and trends in cyberspace. USCYBERCOM has established interagency coordination processes to foster intelligence sharing between the headquarters directorates and other US government entities.

As a functional combatant command, USCYBERCOM has the authority to engage directly with foreign partner equivalents as well. USCYBERCOM has deployed liaison officers to key foreign partners, and is crafting agreements to broaden collaboration and interoperability. Strengthening our foreign partnerships has paid dividends in recent years by increasing our capabilities and capacity. Command elevation will allow USCYBERCOM to mature such partnerships, building relationships and trust that will help us and our partners in shaping the cyberspace domain. We note here our support for the provision (Sec. 1239A) in the NDAA for FY18 that would boost cybersecurity cooperation with NATO and European partners to thwart malign influence by Russia.

USCYBERCOM performs the third of its major missions by enabling Joint Force commanders to deliver the effects they require in and through cyberspace. We see an ever-increasing demand from the Combatant Commanders for support; cyber effects ensure the Joint Force can project power, enhance its lethality, and defend its command and control. Our Joint

Task Force Ares has given important supporting fires to USCENTCOM and USSOCOM in the campaign to defeat ISIS on the ground in Iraq and Syria. We learned many lessons from that fight, particularly regarding intelligence in the battlespace and the broad applicability of traditional targeting processes in the cyber domain. Perhaps the most important takeaway from our experience was how to build the right processes to integrate cyberspace operations as one piece of a complex and coordinated multi-domain military campaign. I have directed our components to apply these and related lessons as we transition our temporary, joint task force model for fighting ISIS in cyberspace to an analogous and enduring construct that addresses the threat of violent extremism worldwide.

In supporting Joint Force commanders, USCYBERCOM is working to synchronize the planning and operations of cyber forces as "high-demand/low density" assets. Two Secretaries of Defense have now endorsed this change in how our cyberspace assets are managed. The new construct provides the Commander of USCYBERCOM the authority to balance risk across the Joint Force by focusing cyber capacity where it is most needed, both in time and space. This strategic approach to military cyberspace assets will allow us to deter and respond to or preempt cyber threats in all phases of conflict and to synchronize cyberspace operations globally. We are building this concept into USCYBERCOM's operational and contingency plans.

The Chairman of the Joint Chiefs of Staff furthered this goal by updating the cyberspace operations command and control framework last fall, directing that USCYBERCOM establish Cyber Operations - Integrated Planning Elements (CO-IPEs) at each Combatant Command. We hope to have all of these new units at full operational capability within the next five years to plan, synchronize, integrate, and de-conflict cyberspace operations with Combatant Command plans and operations. CO-IPEs will be in direct support to Combatant Commanders but will remain under my command and under the administrative control of USCYBERCOM's Service components. USCYBERCOM is leading the planning effort to establish the CO-IPEs. The size and configuration of the CO-IPEs will naturally vary to best fulfill the mission requirements of their host commands; in most cases they will have fewer than 40 people. USCYBERCOM will monitor the Services' progress in standing up their respective CO-IPEs and provide guidance to synchronize their efforts.

Success in our missions depends on a trained and ready force. It sounds unoriginal to call people our most valuable resource, but for USCYBERCOM that old saying is true. I must thank Congress for recently increasing our agility in shaping our workforce; the new Cyber Excepted Service will help us recruit, manage, and retain cyber expertise in a highly competitive talent market. We are rapidly preparing to bring in talented people. With support from the NDAA, the Services have the ability to directly commission cyberspace operations officers, the first of whom will be entering the force early this year. As for our valuable civilian technical experts, we are using the ability to directly hire uniquely skilled people to strengthen our team. I also note that the Services will lead the cyber training mission in FY19 as they take over the training functions that USCYBERCOM has performed in recent years. We have been preparing for that development for some time, and believe the transition will be seamless.

USCYBERCOM's success in cyberspace reflects a total force effort with fully integrated Reserve and National Guard cyber warriors who are trained to the same joint standard as the regular force. In our headquarters at Fort Meade, we employ more than 300 full-time and part-time reservists, providing support for intelligence, operations, planning, training, and cyber capability development. An additional more than 150 Reserve and National Guard members mobilize continually to lead and execute operations in support of CNMF and Joint Task Force Ares. The Reserve Component is especially valuable because Reservists often bring cyber skills from the private sector; many others come to us with insights from extensive federal or state government experience. In addition, the U.S. Army's Reserve and National Guard are building 21 Cyber Protection Teams (CPTs), with plans to reach full operational capability by FY24. These Reserve Component Soldiers are in the fight today. For example, an all-Army National Guard team named Task Force Echo is made up of Soldiers from seven states and has been on-mission since last year, providing essential cyberspace support to our operations.

By the end of this summer, three National Guard and Reserve teams will achieve full operational capability. While that number in itself appears small, the Reserve Component's strength lies within its surge capacity. A significant portion of the Air Force Cyber's contribution will draw on more than a thousand Reserve Component members.

Recent events illustrated a need for improved coordination between Active Duty and Reserve Component cyber forces for domestic response. Future training partnerships between USCYBERCOM, the Reserve Component, state, local, and tribal governments, along with interagency partners, enable these core missions by empowering operations that target the threat outside the United States while allowing law enforcement and state authorities to defend against the threat within the homeland.

Making all this work will require sustained training and exercises. USCYBERCOM personnel, both Active Duty and Reserve Component, hone their skills and their teamwork through increasingly realistic exercise scenarios and simulated network environments. This June, we will re-focus our annual CYBER GUARD exercise from certifying tactical teams to validating our operational concepts. This year's planning takes account of state governors' and National Guard Adjutant Generals' concerns about protecting critical assets. It will be a true operational-level command exercise. Both our CYBER GUARD and CYBER FLAG will include more players from the other Combatant Commands, as well as whole-of-government and industry participants to evaluate cyber capabilities in a Defense Support to Civil Authorities scenario involving foreign intruders in the nation's critical infrastructure. We have synchronized our efforts with the Chief of the National Guard Bureau and his CYBER SHIELD exercise as well as with our DHS partners and their CYBER PRELUDE exercise. Our exercises, moreover, have each year included a wider range of foreign partners in offensive and defensive cyber operations.

Finally, we also need to give good people good tools. In this regard, we are using our new acquisition authorities (conferred in the NDAA for FY16), and executed our first such acquisition when we awarded a contract for IT executive research services in September 2017. The award was valued at over $500,000 and demonstrated that USCYBERCOM can acquire services and capabilities required to equip the Cyber Mission Force. Moreover, USCYBERCOM also delivered the first of several foundational tool kits enabling the CMF to work against adversary networks while reducing risk of exposure; its organic development team equipped JTF-Ares with capabilities to disrupt and influence adversary use of social media. We

also thank the Congress for the provisions of the NDAA for FY18 (Sec. 1642), which requires USCYBERCOM to evaluate new, faster, and more agile development processes for cyber capabilities. We have a team focused on this task, and they should be ready to report their findings to the Secretary within the period stipulated in the Act.

Conclusion

Thank you again for inviting me to appear before you today to represent U.S. Cyber Command, and for all the times you have allowed me to do so over the past four years. Serving as Commander of USCYBERCOM has been the highlight of my military career. The Command has accomplished a great deal in the last four years, operationalizing the cyber mission space and making what seemed nearly impossible in 2014 look almost routine in 2018. Indeed, I have seen dramatic progress in just the past year as the Command matures and prepares for unified combatant command status. All this has been achieved because of the extraordinary talents and efforts of the men and women of USCYBERCOM and those of our mission partners. They are great people, and you should be so proud of them.

Your support has been of enormous help to the Command's maturation, and remains vital to the work that we perform on behalf of our nation. As you have surely gathered from my comments, we have big tasks ahead of us, and your continued assistance could make the difference between mission success and less satisfactory outcomes. I am confident in the ability and the drive of our people to accomplish the tasks before them, just as I have never wavered in my trust in your support for USCYBERCOM. And now I look forward to your questions.

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

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: 29 January 2016

STATEMENT OF

MR. KENNETH RAPUANO

ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE

AND GLOBAL SECURITY

AND PRINCIPAL CYBER ADVISOR

TESTIMONY BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

APRIL 11, 2018

Thank you Chairman Stefanik, Ranking Member Langevin, and Members of the Committee. It is an honor to appear before you alongside Admiral Rogers, Commander of U.S. Cyber Command, to discuss the Department of Defense's (DoD's) priorities in cyberspace. I am testifying today in my roles as Assistant Secretary of Defense for Homeland Defense and Global Security and as Principal Cyber Advisor to the Secretary of Defense. In these roles, I oversee the development and implementation of the Department's cyber strategy and policy with regard to cyberspace; lead the Department's interagency cyber coordination efforts; advise the Secretary and the Deputy Secretary on cyberspace activities; and ensure that the Department's cyber forces and capabilities are integrated across the Joint Force to support the missions assigned by the President to the Secretary of Defense.

The United States faces a complex global security environment characterized by disorder and challenges to the free and open international system. We are in the midst of a long-term strategic competition with two revisionist powers, China and Russia, who seek to shape a world consistent with their authoritarian model. At the same time, U.S. military superiority is increasingly contested in every operating domain by competitors who are fielding capabilities aimed at the battle networks and

operational concepts which underpin Joint Force power projection. Finally, the arrival of the cyber era means that the United States homeland is no longer a sanctuary. State and non-state actors now have the ability to carry out malicious cyberspace activity against U.S. political, economic, and security interests without ever having to cross our borders.

The Department's primary mission is to provide combat-credible military forces to deter and win wars and protect the security of the United States. To that end, DoD cyber forces must ensure that the Joint Force can operate in a cyber-contested environment, support Joint Force lethality with cyber capabilities, and deter or defeat strategic cyber-attacks against the homeland.

Accomplishing these missions requires DoD to be ready to fight in and through cyberspace against a great-power competitor. The Department must maintain the ability to gain access to foreign networks and systems, collect information, and, when necessary, deliver effects in and through the cyberspace domain. The 2018 National Defense Strategy provides a prioritization framework for cyber missions that amplifies its three themes: increasing lethality, strengthening alliances, and reforming the Department's practices. Our end goal is the successful integration of

cyber operations across the Joint Force and throughout all the Department's core missions rather than the sidelining of those capabilities as a niche for a specialized cadre of technical experts.

Cyber security is inherently a team sport. Cybersecurity experts estimate that some 90 percent of cyber-attacks could be defeated by better implementation of basic cyber hygiene practices and best practice sharing. Through basic cyber hygiene and information sharing across the government and private sector, we can drastically decrease the opportunities for our adversaries to hold us at risk. In turn, as we increasingly spend less time countering malicious cyber activity directed against us, we commit more time and resources to developing capabilities to hold our adversaries at risk.

Defending the Joint Force

Defending DoD networks, systems, infrastructure, and information is essential to ensuring the Joint Force can operate in a cyber-contested environment. A successful defense requires the Department to be able to operate in our adversary's cyber-attack infrastructure to preempt, blunt, or halt attacks. DoD also protects its systems and networks by implementing cyber resiliency measures such as hardening against cyber-attacks and

ensuring mitigations have been developed that allow continued functioning when a cyber-attack does occur. If and when the Department detects malicious cyber activity within its networks, DoD's rapid-response capabilities can be brought to bear to secure its networks and systems by halting the cyber adversaries.

Defending the Department's networks also requires identifying and mitigating our own vulnerabilities. As a Department, we recognize that we rely heavily on cyber-enabled critical infrastructure to conduct our core missions and appreciate congressional efforts to expand and strengthen vulnerability identification programs. We are improving and broadening our risk-management framework to assess threats across the Joint Force and allow us to prioritize the mitigation and remediation of our most critical vulnerabilities. We are also moving forward to assess and readdress major weapon systems and critical infrastructure vulnerabilities as mandated by Section 1647 of the National Defense Authorization Act for Fiscal Year 2016 and Section 1650 of the National Defense Authorization Act for Fiscal Year 2017.

Protecting DoD information residing in the Defense Industrial Base (DIB) is critical to enabling Joint Force military overmatch. The wartime

cybersecurity of our systems and networks will mean little if the qualitative advantage of our weapons platforms has been eroded during peacetime by the exfiltration of sensitive military information. The Department must more effectively compete with and challenge cyber actors who are stealing United States defense information by being more proactive and creative in how we leverage counterintelligence authorities to combat information theft.

Ensuring that DoD contractors maintain adequate cybersecurity standards is also critical to protecting the Department's information. In October 2016, we updated the Defense Federal Acquisition Regulation Supplement (DFARS) to require contractors to provide "adequate security" for covered defense information that is processed, stored, or transmitted on the contractor's internal information system or network. We are continuing to evaluate our mandated cybersecurity standards for DoD contractors and working to protect our information outside of Department networks.

Beyond the DIB, we are advancing our understanding of the degree to which Joint Force operations are reliant on civilian defense critical infrastructure (DCI). Much of our warfighting capabilities are dependent on an array of municipal utilities, national utilities, private telecommunications companies, transportation networks, and other assets that are not

connected to our networks and over which we have limited visibility and control. DoD's Mission Assurance process provides a way for us to systematically and thoroughly examine these dependencies and the risks to our military and civilian infrastructures, networks, and systems. We are working to prioritize civilian DCI assets by their criticality to the Department's priority missions so that we can mitigate those risks and build resiliency across all domains, including cyberspace.

Enhancing Joint Force Lethality

DoD is moving to normalize the consideration of cyber capabilities throughout Joint Force operations and contingency planning in order to fully integrate maneuver in the cyberspace domain with maneuver in the physical domains. Cyber capabilities provide commanders with unique tools that have different characteristics than conventional weapons. We must experiment now with innovative ways to pair cyber with other military capabilities to ensure that the Joint Force remains at the forefront of operational proficiency in this new warfighting domain.

Defending the Nation

Defending the nation is a core mission of the Department of Defense and just as we develop military forces, capabilities, and plans to project

power to meet threats from land, air, and sea, we must also be prepared to do so in cyberspace. In this way, the Department is focused on preparations to defend the United States by halting or degrading strategic cyber-attacks using cyber effects operations, as well as developing a range of response options. Additionally, we seek to leverage the Department's extensive information collection mechanisms to provide timely indicators and warnings (I&W) to public and private network and system owners and operators both broadly to enhance our collective preparedness against cyber threats, as well as specifically, so that they can raise their cybersecurity posture if an attack is imminent. DoD runs three of the six Federal cybersecurity centers, which participate in the Enhanced Shared Situational Awareness Initiative (ESSA). I&W information is a two-way street. We want to ensure mechanisms are in place for public and private sector partners to inform us of malicious cyber activity taking place in their networks and systems so that we can potentially address the threat at its source.

Deterrence in Cyberspace

DoD uses "cyber deterrence" to refer to actions taken to convince adversaries not to conduct destructive or destabilizing malicious cyber

activity against the United States However, to date, the United States' limited responses and inconsistent messaging have been ineffective at halting cyber behavior we consider unacceptable. This is challenging – absolute deterrence – or a complete elimination of all malicious cyber activity is unlikely, since cyber weapons are quite unlike nuclear weapons; however, more can and should be done to strengthen our deterrence posture.

The President recognized the importance of a stronger deterrence posture in the 2017 Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," which directed the development of a whole of government approach to deterrence, which was just recently completed. Consistent with these recommendations, and the 2017 report from the Defense Science Board Task Force on Cyber Deterrence, we are implementing a range of actions to improve our ability to deter our adversaries in cyberspace. First, the Department is working alongside other U.S. departments and agencies to develop tailored deterrence plans aligned against specific threats and types of malicious cyber activity. In this way, DoD will contribute to a national-level effort, driving planning and assessment activities for such adversary-focused plans, as well as refining military options, forces, and authorities

that can be leveraged to advance our national interests and contribute to stability and security in cyberspace. Second, the Department is strengthening our ability to operate in a cyber-contested environment, as previously discussed, through ongoing cyber vulnerability assessments of major weapon systems and critical infrastructure and through the effective use of Combatant Command exercises and wargames. The results of these cyber vulnerability assessments, exercises, and wargames will inform risk-based decisions on the most effective way to improve the capability of DoD forces to operate in a cyber-contested environment. Lastly, the Department's Fiscal Year 2019 budget supports U.S. Cyber Command's role to train and equip the Cyber Mission Force with acquisition efforts focused on the four capability areas of: Joint Access Platforms, Joint Tools, Joint Analytics, and Joint Common Services. These investments in foundational capabilities combined with the broader U.S. government's efforts to enhance the cyber security of the most vital U.S. critical infrastructure will substantially bolster the U.S. cyber deterrence posture.

I acknowledge that the Department's report on deterrence strategy to the Congress is long overdue. I continue to work with Department leaders and interagency partners to refine and enhance our deterrence posture and

to present the comprehensive and substantive response your questions deserve.

Building a Cyber Force

One of the Department's most significant cyber accomplishments has been the creation of the Cyber Mission Force (CMF). With more than 6,000 soldiers, sailors, airmen, Marines, and civilians the CMF's ranks include some of the brightest and most talented men and women serving in in the Department. The force is on schedule to complete full force generation before the end of the fiscal year, reflecting the successful completion of a multi-year train-and-equip effort. The current CMF benefits from significant contributions from the Reserve Components, which are being further developed in the near future. We are leveraging the Total Force to meet the Department's needs while promoting strong relationships with state and local authorities that allow our cyber warriors to maintain their ties with their communities even as they contribute to the defense of the Nation.

Reaching completion of the force generation phase is an important step for the CMF and is a testament to the hard work of the Military Departments that have built these forces. As we approach this milestone

before the end of this fiscal year, our focus has increasingly shifted to enhancing readiness with an emphasis on training and capability development. Military operations in cyberspace continue to provide U.S. forces with operational experience as well as insights into the command and control capabilities required to effectively conduct integrated cyber operations. Specific activities aligned with training the CMF include the acquisition of a Persistent Cyber Training Environment (PCTE) and the effective leveraging of existing Joint and Service cyber training capabilities. In addition, we are procuring new capabilities to be more ready in and through cyberspace. With continued congressional support, we will provide our Nation with an agile and war-winning cyber force.

The Department is also moving forward with developing the civilian cyber workforce with the September 2017 launch of the Cyber Excepted Service (CES), an enterprise-wide approach to managing the civilian cyber workforce. CES provides the Department with the agility and flexibility to identify, recruit, develop, and retain the very best cyber professionals. It helps the Department streamline hiring procedures to fill critical cyber positions quickly across the enterprise by providing hiring managers with more options for sourcing candidates and allowing them to offer more competitive compensation packages. I thank you and the other members

of Congress who have supported the efforts to provide the Department the hiring and managing authorities and the means to provide the world's best training to our cyber forces. We are monitoring these programs closely to ensure that we have the right mix of tools available to cultivate the workforce necessary for this 21st Century domain and we will report back to you on the effectiveness of our efforts.

Allies and Partners

The cybersecurity efforts of our allies and partners are critical to protecting ourselves from malicious cyberattacks. By establishing and cultivating international partnerships, the Department increases its capacity to detect, monitor, prevent, and defeat threats in cyberspace while working to ensure that our allies and partners develop and build strong cyber defense capabilities. Security cooperation activities in general, and cybersecurity cooperation activities in particular, provide an opportunity for the United States and the Department to improve and leverage the cyber capabilities and capacity of our allies and partners so they are able to help us shape the strategic environment in favor of U.S. national objectives.

Working with our allies and partners is also critical to establishing and enforcing responsible state behavior in cyberspace, giving strength to

shared rules of the road for stability and security in cyberspace. We are more effective when we stand shoulder to shoulder with our friends when calling to account those who act maliciously and recklessly by attacking the interconnected information and infrastructure that makes up cyberspace. The Department's security cooperation authorities will be helpful in developing the cyber capabilities of our allies and partners so that they are more effective at protecting their systems and engaging alongside us against our common adversaries. Although norms are unlikely to restrain the most malicious, persistent adversaries in cyberspace, they provide standards for responsible states, giving context to justified proportional response. Standing together with our like-minded allies and partners, we can increase the costs to those adversaries insisting on continuing malicious cyber activities that fall outside the norms of acceptable behavior.

Reforming Business Practices

The Department has been justly criticized for a bureaucratic culture that often prioritizes exacting thoroughness and minimizing risk over speed and innovation. We are optimized to deliver exquisite solutions developed over lengthy periods of time rather than immediate, perhaps imperfect solutions that can be improved iteratively. Our current approach is

particularly problematic in the cyberspace domain, where the most successful technology companies have adopted development models that revolve around rapid prototyping and rapid deployment followed by frequent and incremental updates. The Department is committed to ensuring that our cyber forces are able to leverage capability development processes that can deliver effective results in a timely manner. One of our efforts, outlined in Section 1642 of the National Defense Authorization Act for Fiscal Year 2018, is to ensure our cyber acquisition practices are as streamlined, agile, and efficient as possible in order to deliver the right tools rapidly to our warfighters.

Organizing for Success

U.S. Cyber Command has been given Service-like responsibilities that will allow it to acquire cyber-unique equipment and technology rapidly and to train its people to meet the latest threats. This is absolutely critical for an agile command responsible for maintaining the Joint Force's advantages in cyberspace. This Command is now functioning as an operational command while supporting other Combatant Commands by providing cyber operational planning and cyber effects. We can be very proud of the men and women who have worked tirelessly to make this

happen. I will continue to work closely with Admiral Rogers and, assuming confirmation Lieutenant General Nakasone, as U.S. Cyber Command approaches full operational capability to ensure that it has the powerful advocate it needs to continue its success.

The Department is developing the organization, processes, and procedures that will support the command as it becomes more mature and capable. The Department is developing options to meet the intent of Sections 902 and 923 of the National Defense Authorization Act for Fiscal Year 2017 (NDAA for FY 2017) and Sections 909, 1635, and 1637 of the NDAA for FY 2018. We continue to refine these options by assessing the Department's missions in and through cyberspace, considering the future environment, and analyzing the benefits and risks to optimize roles and responsibilities to ensure that the Department is best postured for this challenging and rapidly changing domain of warfare. I look forward to working with you and other members to structure the Department's approach to provide the appropriate military department secretary-like oversight and ensure that adequate guidance and support are provided to the newly elevated command.

Conclusion

I thank the subcommittee members for their continuing support of the Department's efforts to develop the cyber capabilities and capacity we need to adjust to the changing character of conflict. The people in our cyber community are the best in the world and I am honored to serve with them. The Department is committed to approaching the development of our cyber capabilities with the sense of urgency warranted by the gravity of threats we face. We have undertaken comprehensive efforts in concert with our interagency allies, partners, and the private sector to improve the Department's cybersecurity posture and to ensure that we have the ability to operate in any domain, at any time, and against any adversary. Our strong relationship with Congress has been a critical component of our success and will remain vital as we continue our work to ensure the Department's cyber forces are prepared to compete, deter, and win against any opponent. To that end, I am grateful for Congress's strong support and particularly this subcommittee's interest in these issues, and I look forward to your questions.

Kenneth P. Rapuano
Assistant Secretary of Defense for Homeland Defense and Global Security

Mr. Kenneth P. Rapuano is the Assistant Secretary of Defense for Homeland Defense and Global Security. Previously Mr. Rapuano was a Senior Vice President at the ANSER Corporation, and the Director of the Studies and Analysis Group which provided multi-disciplinary studies and operational analysis for a broad array of government clients in the national security, homeland security areas. Up until November of 2016, Mr. Rapuano Directed the Homeland Security Studies and Analysis Institute (HSSAI), a Federally Funded Research and Development Corporation (FFRDC) operated by ANSER, a mission oriented not-for-profit organization.

Prior to joining ANSER Mr. Rapuano was the Director of Advanced Systems at the MITRE Corporation. He was responsible for guiding crosscutting strategic national and homeland security mission initiatives, with particular focus on counterterrorism, intelligence, aviation security, crisis management/decision support, national preparedness, and CWMD.

Previously, Mr. Rapuano served at the White House as Deputy Homeland Security Advisor to President George W. Bush from 2004-2006. He was responsible for managing the development and implementation of homeland security policies among departments and agencies, chaired the Homeland Security Council Deputies Committee, and co-chaired the White House Counterterrorism Security Group. He left the White House in 2006 to volunteer for deployment as a Marine Corps officer to Afghanistan with a Joint Special Operations Task Force, establishing and directing a targeting fusion center tracking high-value terrorists and insurgents. He also served in Iraq in 2003, commanding the Joint Interrogations and Debriefing Center of the Iraq Survey Group established to conduct the mission of surveying and exploiting possible weapons of mass destruction activities across Iraq.

In 2003, Mr. Rapuano was appointed Deputy Under Secretary for Counter Terrorism at the Department of Energy, responsible for nuclear counter terrorism, homeland security, emergency response, and all related special access programs for DOE and the National Nuclear Security Administration. Previous to that, he was the National Security Advisor to the Secretary of Energy. Mr. Rapuano has also served as Special Assistant to the Assistant Secretary of Defense, International Security Policy. He served 21 years on active duty and in the reserves as a Marine Corps infantry officer and intelligence officer.

Mr. Rapuano has also served as a Distinguished Research Fellow at the National Defense University's Center for the Study of WMD, as a member of the Defense Science Board Task Force on the Role of DoD in Homeland Defense, the Pacific Northwest National Lab's National Security Advisory Committee, the FBI's Weapons of Mass Destruction Directorate Advisory Group, the DHS Quadrennial Homeland Security Review Advisory Committee, and the DHS Science and Technology Advisory Committee.

Mr. Rapuano received a bachelor's degree in Political Science from Middlebury College, a master's degree in National Security Studies from Georgetown University, and has attended the Marine Corps Air-Ground Task Force Intelligence Officer Course at the Navy and Marine Corps Intelligence School.

WITNESS RESPONSES TO QUESTIONS ASKED DURING THE HEARING

APRIL 11, 2018

RESPONSES TO QUESTIONS SUBMITTED BY MS. STEFANIK

Admiral ROGERS. [The information is for official use only and retained in the committee files.] [See page 11.]

Secretary RAPUANO. A common operating picture requires the Federal government and the private sector to share information rapidly. This means improving processes so that DOD and the intelligence community (IC) can push information to the Department of Homeland Security (DHS) and out to private sector critical infrastructure partners, but also so that those partners can share more threat data from their networks with the Federal government. This information could be critical in helping DOD conduct its mission to defend the homeland. By understanding the threats facing critical infrastructure, we can better prioritize DOD's operational activities. This is a collective responsibility to which both the public and private sectors must contribute.

My staff and I work in close collaboration with the National Security Council staff and our interagency partners at the State Department, DHS, the Federal Bureau of Investigation (FBI), and other departments and agencies to ensure that the Federal Government has the necessary policies in place and is taking appropriate actions to address critical issues and potential threats in cyberspace. Beyond contractual relationships, and both the mandatory and voluntary information-sharing programs DOD has with the Defense Industrial Base, DOD works closely with DHS and the FBI to address threats to critical infrastructure. [See page 11.]

RESPONSES TO QUESTIONS SUBMITTED BY MR. LANGEVIN

Admiral ROGERS. [The information is for official use only and retained in the committee files.] [See page 12.]

Secretary RAPUANO. USCYBERCOM incorporates lessons learned into its mission planning and operations by instituting a real-time review and feedback mechanism during its operations as well as conducting larger scale after-action sessions to identify strategic issues. All individual operations are planned, reviewed, and approved prior to execution by independent, senior-level technical advisors who provide guidance and modifications based on their experience and extensive knowledge.

Once an operation is complete, the same individuals review and critique whether the operation was conducted according to plan and if any unanticipated challenges arose during execution. If a mistake occurs during the course of the operation, the senior technical advisors have the opportunity to determine whether the operator requires additional training or whether the mistake was due to a simple error. USCYBERCOM personnel also often conduct "hot washes" (debriefing meetings) on their strategic operations with senior leaders to identify the lessons learned and to propose recommendations for improving future operations. These recommendations can include resource shortfalls, process requirements, and decision-making efficiencies to be gained.

Lessons learned from operational employment of the Cyber Mission Force (CMF) are being routinely captured and integrated into ever-evolving curriculum. The Department of the Army, for example, is comparatively in the best position to ensure that it is able to leverage and institute "lessons learned" from real-world Cyberspace Operations and evolve curriculum, training, and recertification processes rapidly. The Army's decision to have its institutional CMF workforce collocated with a majority of its operational CMF workforce gives the Army a significant advantage in accessing, educating, training, developing, employing, and retaining this workforce.

The decision to establish the U.S. Army Cyber School at Fort Gordon, Georgia, was made, in part, to co-locate the institutional and the operational force. Benefits of this colocation include, but are not limited to, gaining synergy across both workforces through shared experiences, the ability to take lessons learned and turn them rapidly into appropriate adjustments to the curriculum, an ability to "re-fresh" instructors while they are still serving in instructor billets, an ability rapidly to establish critical training that is more immediately available to a large portion of the operational force, and an ability to extend the "Schoolhouse" learning environment by introducing students to the operational environment while they are still in train-

ing. Additionally, as the U.S. Army Cyber School began constructing curriculum specifically to meet the needs of its CMF, it turned to cloud-hosted storage and synchronization solutions that allow qualified members of the CMF to "crowdsource" on the curricula for both rapid creation and continual maintenance. To date, more than 100 contributors have worked to provide almost 7,000 updates to courseware through their chosen distributed version-control system.

During the establishment of the Joint Cyber Mission Force, the initial emphasis was simply on building the 133 teams across the Military Services and thus the Initial Operating Capability (IOC) and then Full Operating Capability (FOC) of the Joint Cyber Mission Force. Reporting by the units focused on rudimentary reporting of total personnel assigned to the teams against a percentage of personnel assigned to key work roles and their associated levels of training and certification.

These teams are trained to deter and defeat strategic threats to U.S. interests and infrastructure, ensure DOD mission assurance, and achieve Joint Force Commander objectives. Accordingly, as we move forward, DOD recognizes the need to work with USCYBERCOM and the Military Services to effect joint standard reporting requirements and standards for both "Capacity" and "Capabilities." As the Department resources and equips these teams with cutting-edge cyber tools, accesses, and platforms to protect against sophisticated cyberattacks and to ensure deterrence and military advantage in and through cyberspace, enhanced CMF Readiness reporting that assesses "Capacity" readiness across the Military Services to a common joint standard by measuring not only Personnel and Training, but also Equipment and Supplies and Condition of Equipment, will result in more deliberate and objective measures of force readiness. In addition, the Department needs to work with USCYBERCOM and the Military Services to effect "capabilities-based" reporting against Mission-Essential Tasks that reflect fundamentals based on unit design and organization. [See page 12.]

RESPONSE TO QUESTION SUBMITTED BY MRS. MURPHY

Admiral ROGERS. [The information is for official use only and retained in the committee files.] [See page 16.]