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.