STATEMENT OF

ADMIRAL MICHAEL S. ROGERS

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

SENATE COMMITTEE ON ARMED SERVICES

9 MAY 2017

Chairman McCain, Ranking Member Reed, and Members of the Committee, thank you for your enduring support and the opportunity today to represent the hard-working men and women of United States Cyber Command (USCYBERCOM). I welcome the opportunity to describe how USCYBERCOM leads Department of Defense (DoD) efforts in the cyberspace domain and supports the nation's defense against sophisticated and powerful adversaries.

The Department of Defense recognized seven years ago that the nation needed a military command focused on cyberspace. USCYBERCOM and its subordinate elements have been given the responsibility to direct, operate, and secure the Department's systems and networks, which are fundamental to the execution of all DoD missions. The Department and the nation also rely on us to build ready cyber forces and to be prepared to employ them when significant cyber-attacks against the nation require DoD support.

USCYBERCOM has been a sub-unified command under U.S. Strategic Command (USSTRATCOM) since its creation in 2010. The command includes six operational-level headquarter elements, assisted by U.S. Coast Guard Cyber, a component of the Department of Homeland Security (DHS). USCYBERCOM's action arm is the Cyber Mission Force (CMF), which comprises 133 teams and is continuing to build to a total of approximately 6,200 military and civilian personnel. All of those CMF teams reached at least initial operational capability in 2016. Many have attained full operational capability (FOC), and I expect all of them will attain FOC status by 1 October 2018, just 15 months from now.

I want to update you on our initiatives and plans for that time to come. Our three lines of operations are to provide mission assurance for DoD operations and defend the Department of Defense information environment; to support joint force commander objectives globally; and to deter or defeat strategic threats to U.S. interests and critical infrastructure. We conduct full spectrum military cyberspace operations to enable actions in all domains, ensure US and Allied freedom of action in cyberspace, and deny the same to our adversaries. I have asked that our Command and its components focus their efforts in several areas to ensure we can accomplish missions, both now and in the future. Defense of DoD information networks remains our top priority, of course, and will move this beyond a network focus to one that includes weapon systems/platforms and data. We will also continue progress on the CMF build and attainment of FOC for all teams, while increasing the CMF's readiness and its ability to hold targets at risk. We will posture the CMF to deliver effects across all phases of operations; to improve operational outcomes by increasing resilience, speed, agility, and precision; to generate operational outcomes that support DoD strategy and priorities; to create a model for successful Reserve and National Guard integration in cyberspace operations; and finally to strengthen partnerships across the government, with our allies, and with the private sector.

Your strong and continuing support is critical to the success of the Department in defending our national security interests, especially as we comply with the recent National Defense Authorization Act directive to elevate USCYBERCOM to unified combatant command status. As you well know, I serve as both Commander of USCYBERCOM and Director of the National Security Agency and Chief, Central Security Service (NSA/CSS). This "dual-hat" appointment underpins the close partnership between USCYBERCOM and NSA/CSS—a

significant benefit in cyberspace operations. The institutional arrangement for providing that support, however, may evolve as USCYBERCOM grows to full proficiency in the future, as I shall explain below.

The Cyber Threat Environment

The pace of international conflict and cyberspace threats has intensified over the past few years. We face a growing variety of advanced threats from actors who are operating with ever more sophistication and precision. At USCYBERCOM we track state and non-state adversaries as they continue to expand their capabilities to advance their interests in and through cyberspace and try to undermine the United States' national interests and those of our allies.

America faces multiple challenges from non-state cyberspace actors who impact our citizens and our economy, which now depends on trusted data. For instance, over the last year we have seen increased use of ransomware against individuals and businesses who find their data locked and are forced to pay in order to regain control of their files and intellectual property. Such threats primarily fall under the jurisdiction of law enforcement authorities, particularly the Federal Bureau of Investigation and the Secret Service. Nevertheless, criminal actors become a military concern when malicious state cyber actors pose as cyber criminals, or when cyber criminals support state efforts in cyberspace. This means that we take notice when cybercriminals employ tactics, techniques and procedures used by state adversaries.

My main concern relates to state-based cyber actors, whose malicious activities have only intensified since I spoke to this Committee last year. As we have seen, cyber-enabled destructive and disruptive attacks now have the potential to affect the property, rights, and daily lives of Americans. We are particularly concerned as adversaries probe and even exploit systems used by government, law enforcement, military, intelligence, and critical infrastructure in the United States and abroad. We have seen states seeking to shape the policies and attitudes of democratic peoples, and we are convinced such behavior will continue for as long as autocratic regimes believe they have more to gain than to lose by challenging their opponents in cyberspace.

At the operational level of conflict, states are incorporating cyber effects to support their military operations. As early as 2008, for instance, the Russian incursion in Georgia was accompanied by a denial-of-service attack against Georgia's government Internet services as well as the defacement of content on official web pages. We are not yet seeing true, combined-arms operations between cyber units and "kinetic" missions, although we have spotted hints of this occurring in Syria and Ukraine as the Russians attempt to boost the capabilities and successes of their clients and proxies. In general, these and other conflicts feature cyber operations by all sides; Russian government sites, for example, have sporadically been attacked by sympathizers from Ukraine. Advanced states continue to demonstrate the ability to combine cyber effects, intelligence, and asymmetric warfare to maintain the initiative just short of war, challenging our ability to react and respond. Further, states clearly continue to leverage cyberspace to conduct significant, widespread, intelligence operations. Access to large volumes of data enable Insider threats; defending against these is a critical requirement of the current and future landscape.

U.S. Cyber Command has seen indications that several states are investing military resources in mining the networks of the Department of Defense and its contractors. On a daily basis, state cyber actors coordinate and execute exploits and scans of the DoD Information Networks (what we now call the DoDIN) as well as related governmental and private systems. These activities are often automated, and they can include well-crafted spear-phishing expeditions. We assess that the motivation behind these efforts is predominantly espionage, but the mere possibility that an adversary might establish a persistent presence in DoD networks is always a grave concern; such intrusions, when they occur, are quite disruptive and expensive to remediate.

A still-greater concern is the persistence of adversary attempts to penetrate critical infrastructure and the systems that control these services. We assess that several countries, including Iran, have conducted disruptions or remote intrusions into critical infrastructure systems in the United States. Last year, for example, the Justice Department announced indictments of seven Iranians for cyber disruptions of U.S. financial institutions. The Attorney General reported that 46 U.S. companies together suffered tens of millions of dollars in losses as a result of the attacks. In addition, in late 2015 a malware tool (Black Energy) identified in energy-sector systems worldwide was implicated in a malicious cyber attack against Ukrainian power systems. The Department of Homeland Security has been warning systems administrators at critical infrastructure sites in the United States and abroad about sophisticated cyber threats from malicious actors employing Black Energy. In December 2015, the cyber actors who had deployed Black Energy in Ukraine briefly cut off electricity to hundreds of thousands of Ukrainians, possibly in support of Moscow's aims in Crimea and Eastern Ukraine. Infiltrations in US critical infrastructure—when viewed in the light of incidents like these—can look like preparations for future attacks that could be intended to harm Americans, or at least to deter the United States and other countries from protecting and defending our vital interests.

Violent extremist organizations constitute another focus for USCYBERCOM. For over a decade, they have used the Internet to publicize their malicious actions to intimidate opponents and win sympathizers. As we know from the reporting and analysis of respected journalists and think tanks, groups like ISIS conduct sophisticated multi-media campaigns that spread its messages swiftly and globally. While ISIS uses the Internet to recruit followers and solicit contributions in the West, its media campaign also effects viewers closer to home in the Middle East, boosting morale among ISIS fighters, frightening opponents, and promoting the false narrative that the Arab future inevitably belongs to a radical Salafist brand of Sunni fundamentalism. This information campaign through cyberspace has directly and indirectly impacted Americans, inciting attacks on Americans and the citizens of our European allies, who have suffered even worse assaults than we have seen here. Legitimate Internet media outlets obviously have no interest in lending social spotlights to terrorists by hosting violence or propaganda material, and regularly remove these messages and advertisements when they spot them (or the content is brought to the companies' attention). Yet ISIS is resilient and persistent, and continues to spread its message. In addition, ISIS and other violent extremists communicate over encrypted channels to maintain command and control of their operatives and forces.

Examples like these foretell an uncertain future. Several trends could complicate it still further, like the growing "Internet of Things" providing millions of new Internet-connected devices for adversaries to exploit. Today, consumers who can hardly keep up with patching their laptops and updating their cellphone operating systems are wondering how to upgrade the firmware on their home security cameras or Wi-Fi extenders to keep their families and homes from being victimized by malicious cyber actors. Technological developments are outpacing laws and policies, and indeed will have long-term implications that we have only begun to grasp.

US Cyber Command in Operation

Hardly a day has gone by during my tenure at USCYBERCOM that we have not seen at least one significant cyber security event occurring somewhere in the world. This has consequences for our military and our nation at large. I want to reiterate what I told this Committee last year: every conflict around the world now has a cyber dimension. "Cyber war" is not some future concept or cinematic spectacle, it is real and here to stay. The fact that it is not killing people yet, or causing widespread destruction, should be no comfort to us as we survey the threat landscape. Conflict in the cyber domain is not simply a continuation of kinetic operations by digital means, nor is it some Science Fiction clash of robot armies. It is unfolding according to its own logic, which we are continuing to better understand. We are using this understanding to enhance the Department's situational awareness and manage risk. In light of this trend, I am convinced that we as a nation created our own military capability in cyberspace not a moment too early. Our government and military have gone from wondering whether we have a systemic computer security problem to recognizing that the problem can spread in seconds.

Let me explain how our Department of Defense cyberspace capability has progressed at USCYBERCOM over the last year. The Cyber Mission Force attained initial operational capability, with the last team reaching this milestone in October 2016. Our component commanders are moving out to ensure our people get training and certifications required to reach full operational capability for each CMF team. Achieving FOC, however, is not the ultimate goal. We must ensure the CMF also achieves and sustains a high level of readiness, just like any other military force.

My first mission priority as Commander of USCYBERCOM remains the defense of the DoD information network, which encompass millions of network devices, hundreds of thousands of users, well over ten thousand network enclaves, the data they carry, and the networked technology embedded in weapon systems and other operational platforms. Real-world defensive cyberspace operations have sharpened USCYBERCOM's ability to detect, confine, and eradicate threats from DoD networks and systems. At the same time, adversary cyberspace operations have grown more sophisticated and assertive, resulting in intrusions that have strained the abilities and capacity of DoD cyber forces. With broad authorities to operate within DoD networks, USCYBERCOM has been able to experiment with operational models and tradecraft, improving the effectiveness and efficiency of defensive missions. Our techniques are being adopted and refined across the force, making intrusion response more predictable and effective. USCYBERCOM has improved DoD network defenses through the implementation of new

authorities, innovative command and control structures, and operations informed by offensive planning and intelligence (particularly signals intelligence).

USCYBERCOM executes its DoDIN defense mission in part through Cyber Protection Teams (CPTs)—the defense-focused forces within the CMF. These teams have real-world experience dealing with sophisticated intruders in DoD systems. The CPTs conduct internal defensive measures to protect key DoD terrain in cyberspace, coordinating with local defenders in the cybersecurity service providers, including those aligned to USCYBERCOM under Global Force Management guidance. The CPTs work with system owners, administrators, and local network defenders to find vulnerabilities and hunt for intruders inside DoD networks. This approach embodies the Department's shift to an operational mindset. Should adversary activity be detected, CPTs track, confine, and expel malicious actors using time-tested doctrinal principles consistent with those employed in the other domains. CPTs share what they learn with other network defenders, offensive operations planners, and the Intelligence Community. USCYBERCOM's continual efforts to adapt to the shifting threat environment have resulted in considerable gains to DoDIN security and resiliency.

In addition, as the operational sponsor of the Joint Information Environment (JIE), USCYBERCOM is working with partners to improve the security of the DoDIN. These efforts include implementation of Joint Regional Security Stack (JRSS) enterprise cybersecurity capabilities, integration of IT systems management into the cyberspace operations framework, and development of technical and operational frameworks that will enable establishment of comprehensive cybersecurity practices within DoD and mission partners.

The Defense Information Systems Agency serves as DoD's "Internet service provider" and thus plays a vital role in securing and defending the DoDIN. Its director is dual-hatted as the commander of one of USCYBERCOM's operational components, Joint Force Headquarters (JFHQ)-DoDIN, which is tasked with directing and executing global DoDIN operations and defensive cyberspace operations. This component oversees the Command Cyber Readiness Inspection (CCRI) process in collaboration with local network administrators. CCRIs help JFHQ-DoDIN assess DoDIN systems for compliance with cybersecurity directives and USCYBERCOM orders; inspections thus support USCYBERCOM and DoD Chief Information Officer-led efforts to improve the Department's cybersecurity accountability.

USCYBERCOM works with the Services, NSA and the Defense Cyber Crime Center (DC3) to ensure the CPTs are optimally manned, trained, and equipped. This includes development and acquisition of new capabilities as technology advances; the building of realistic training environments; and resourcing and refining of new models for CPT deployment and operations. USCYBERCOM also seeks to enhance the Department's situational awareness of the status of the DoDIN and adversary activities, to extend protection from the network level down to weapons systems, and to develop capabilities and common approaches for linking cybersecurity risk (beyond compliance) to mission assurance in order to inform warfighting decisions and mitigation efforts.

USCYBERCOM's missions extend far beyond the defense of the DoDIN. In particular, the Command supports the geographical and functional combatant commands in their operations

and missions. This is the business of the USCYBERCOM's Cyber Combat Mission Force. The Cyber Combat Mission Force is the operational-level offensive forces of the CMF, comprising Combat Mission Teams (CMTs) and Combat Support Teams (CSTs), aligned to the Combatant Commands to support their execution of military operations. The CMTs and CSTs are manned, trained, and equipped by their parent services, which exercise oversight of the combat forces they generated through the Joint Force Headquarters (JFHQ) associated with each Service cyber component.

USCYBERCOM is working to synchronize cyber planning and operations across the entire joint force. Since gaining the Secretary of Defense's approval for this proposal in early 2016, USCYBERCOM has implemented a process to allocate limited CMF resources among the commands as "high-demand, low-density" military assets. Currently in implementation, this process will enable USCYBERCOM to balance national and operational-level priorities, enabling the Chairman of the Joint Chiefs of Staff to guide the former through the Command in a crisis while providing tailored capacity forward to support the combatant commands when a situation moves towards actual conflict. USCYBERCOM is also helping the combatant commands build cyber effects into their planning processes so that cyberspace missions are synchronized with operations in the other domains. Indeed, in some situations, USCYBERCOM is the supported command.

Achieving Full Operational Capability in the Cyber Mission Force is our goal, but we acknowledge that reaching that milestone is only a capability metric and not a measure of overall readiness. CMF readiness is a shared responsibility between USCYBERCOM and the Services, and over the last 15 years of conflict we have recognized the costs of continuous operations and seen those costs grow the most in "high-demand, low-density" units – like our CMF teams. We employ teams before they are FOC, which is comparable to employing fighter squadrons before they are fully manned or equipped. Achieving and sustaining readiness is going to require a comprehensive set of solutions, ranging from an agreed upon readiness model between USCYBERCOM and the Services, to ensuring the manpower depth necessary to accommodate professional development, technical proficiency, and career predictability. I am confident we will achieve Full Operational Capability by our 30 September 2018 deadline, but I acknowledge that the true challenge will be sustaining the readiness of the CMF and the remarkable men and women who serve within the teams. We have a duty to them, and we must ensure that they are well trained, prepared, and mission-ready.

USCYBERCOM is executing its missions to support operations against violent extremists, especially across the US Central Command's area of responsibility (and is helping US Special Operations Command's efforts as well). About a year ago, Secretary Carter facilitated this support by issuing an execute order that, among other things, helped USCYBERCOM by authorizing us to "task organize" for specific missions expected to last weeks, months, or longer. The result of this change was a new organization, Joint Task Force (JTF)-Ares, established by me as the Commander of USCYBERCOM in the spring of 2016 to coordinate cyberspace operations against ISIS. JTF-Ares' mission is to provide unity of command and effort for USCYBERCOM and coalition forces working to counter ISIS in cyberspace. The JTF model has helped USCYBERCOM to direct operations in support of

USCENTCOM operations, and marks an evolution in the command-and-control structure in response to urgent operational needs.

JTF-Ares has helped strengthen unity of efforts against ISIS across international coalition and domestic partners, reinforcing USCYERCOM's informal role as a hub for whole-of-government cyber planning and execution against terrorist organizations and targets. Cyber effects can be achieved at-scale and with remarkable synchronization when mission partners share plans, accesses, capabilities, and tactics in support of common objectives. USCYBERCOM, working with the National Counterterrorism Center (NCTC) and the various departments and agencies engaged in this campaign, is using opportunities such as the defeat-ISIS campaign to build trust among operational partners.

USCYBERCOM expects to make progress through 2018 in several key areas. The Command will complete the CMF build, work with DoD partners to equip the CMF, resource and refine command-and-control structures and processes, and develop policies, plans, and operational concepts that support national-level and joint warfighting needs. USCYBERCOM seeks with DoD and Intelligence Community partners to overcome organizational and technological challenges associated with supporting offensive operations at the strategic, operational, and tactical levels. Finally, USCYBERCOM will collaborate with allies and partners to enable collective defense and develop cyber "response actions" that provide options to decision makers from pre-crisis through kinetic operations across all phases of conflict.

Defending the nation in cyberspace is complex in both technical and policy terms. Like all Combatant Commands, USCYBERCOM is authorized only on order from the President (or the Secretary of Defense if the President is unavailable) to defend against a threat to the nation that would qualify as a "use of force" under international law. The Cyber National Mission Force (CNMF) focuses on countering adversaries' malicious cyber activities against the United States and prepares to conduct full-spectrum cyber operations against adversaries when directed. The CNMF is building a force of National Mission Teams (NMTs), National Support Teams (NSTs), and National Cyber Protection Teams (N-CPTs). Partnering with NSA, the CNMF tracks adversary cyber actors to gain advantages that will enable the United States to preclude cyber-attacks against US national interests. The CNMF is working with operational partners to develop and exercise the capabilities and operational concepts needed to enable combined and coalition operations (when authorized) in partnership with other government and appropriate private-sector partners.

USCYBERCOM manages only a portion of the "whole-of-nation" effort required to defend America's critical infrastructure. The Command works with civilian agencies under their authorities to help protect national critical infrastructure and to prepare for scenarios in which US military action to defend the nation may be required.[1] The Command is expanding its ties with the Reserves and the National Guard. Indeed, cyber response teams operating under Guard authorities can perform a variety of missions in support of state, local, and private entities (which operate independently under their own authorities). Recent legislation to incentivize information

[1] The Department of Justice (particularly the Federal Bureau of Investigation) is the lead for cyber-related investigations and law enforcement, while the Department of Homeland Security takes the lead for national protection and recovery from cyber incidents.

sharing will also help the Command and DoD to work more closely with the private sector in mitigating threats outside of government and military systems. The federal government has created a framework for implementing official channels to share information, and clarifying the lanes in the road for US government assistance to the private sector. Whatever USCYBERCOM's ultimate role in that process is determined to be, I continue to tell all audiences that we adhere strictly to the Constitution and law in guarding civil liberties and privacy.

The Command is increasing its efforts in the areas above in alignment with the 2015 *DoD Cyber Strategy*. The Department, as you know, is engaged in a broad effort to improve the security of its information enterprise and to build a culture of cybersecurity. Doing so requires measures well beyond hardening the network architecture, and it cannot be accomplished in just a year or two, even with unlimited resources. The strategy is to replace the old infrastructure, to harden what we are maintaining while increasing its capability, and to grow a workforce possessing outstanding cybersecurity awareness and practices. Beyond that, we must understand that determined adversaries can sometimes bypass even the best security, and thus we must build our skills, as well as an operational mindset, for defeating them in our own networks.

These efforts, of course, depend on skilled, focused, and motivated people in a trained and ready force. USCYBERCOM tapped the expertise of NSA to deliver intensive training for cyber personnel, initially taking the lead in training operators from the Service cyber components who graduate to join the CMF teams. This hybrid arrangement will come to an end, with the Services resuming responsibility and authority for training CMF personnel at the end of 2018. In keeping with DoD's Total Force concept, the Reserve component and the National Guard will also help to build the force. This requires flexibility with organizational requirements and manning standards, but it is already helping to increase the manpower and expertise we can put against some of our most difficult challenges.

USCYBERCOM is maturing its methods for identifying requirements and developing capabilities. The Command last year established a capabilities development team for performing this task, and that group has already done much good. It is doing so not only by working with industry, academia, and other agencies to identify promising ideas, but also in learning how to utilize the data we already generate from our own operations (particularly on DoD systems) to spot useful and/or anomalous patterns. The Command generally lacks NSA's authorities in acquiring the tools for such initiatives, but Congress recently authorized USCYBERCOM acquisition authority for up to $75 million each year through the end of FY2021 to rapidly deliver acquisition solutions for "cyber operations-peculiar" capabilities. We look forward to reporting to the Committee soon on how we are executing this authority.

USCYERCOM has now matured to the point where it brings vital capabilities to the defense of American interests on a daily basis. In light of the increasing severity of cyber threats, Congress in the National Defense Authorization Act for FY2017 directed the President to elevate USCYBERCOM to the status of a full unified combatant command. Elevation implicitly recognizes the importance of cyberspace to our national security. I support this step, although the timing and process for elevation are being worked out within the Department, and we expect to have more details to report to the Committee as they emerge. We will pay particular attention

to the implementation of the Act's provisions regarding authority for the acquisition of "cyber operations-peculiar" capabilities. As you know, the language in this section parallels that granted to US Special Operations Command. USSOCOM's requirements, however, are not always congruent with those to support operations in the cyberspace domain, and thus authorities in the one field might not always be directly analogous to those in other. We are working with Committee staff to ensure that our implementation comports with Congress's intent.

The recent National Defense Authorization Act in a separate provision also described some conditions for splitting the "dual-hat" arrangement, once that can happen without impairing either organization's effectiveness. This is another provision I have publicly stated I support pending the attainment of certain crucial conditions. I have offered this caveat because the challenges in cyberspace are some of the greatest facing America. Meeting tomorrow's threats requires leaders who can devote their time and energy to building the capabilities of USCYBERCOM and NSA while guarding the rights and liberties of US persons protected by our Constitution. We have not yet matured the Command to a point where splitting the two hats would not functionally impair mission effectiveness. If that point is reached on my watch, I intend to keep the Committee fully informed of the conditions set for the split and how they are met.

USCYBERCOM will also engage with this Committee on several other matters relating to the enhancement of the Command's responsibilities and authorities over the coming year. These would include enhancing the professionalization of the cyber workforce, building capacity and developing capabilities, and streamlining acquisition processes. Most or all of these particulars have been directed in recent National Defense Authorization Acts; and along with the Office of the Secretary of Defense for Policy and the Joint Staff, we will be talking with you and your staffs to iron out the implementation details.

Conclusion

Thank you for inviting me to talk with you today about US Cyber Command and its work. The Cyber Mission Force approaching full operational capability, and USCYBERCOM is poised to become a mature unified combatant command. USCYBERCOM personnel are proud of the roles they play in this endeavor, and are motivated to accomplish the many missions assigned to them and overseen by the Congress, particularly this Committee. They work to counter adversaries and support national and joint warfighter objectives in and through cyberspace on a previously unattainable scale and in a sustainable manner. Innovations are constantly emerging out of operational necessity. These, if supported with agile policies, decision-making processes, capabilities, concepts of operation, and command and control structures, will help USCYBERCOM realize its potential to counter adversary cyber strategies in and through cyberspace. The Command's full-spectrum successes have validated concepts for creating cyber effects on the battlefield and beyond. Real-world experiences in meeting the requirements of national decision-makers and joint force commanders have driven operational advances that need time to mature. With the Cyber Mission Force now at initial operational capability, USCYBERCOM is demonstrating its contribution to comprehensive US Government approaches to countering adversary strategies in and through cyberspace.

The men and women of US Cyber Command thank you for your support, both in the past and in the big tasks ahead of us. We understand that a frank and comprehensive engagement with Congress not only facilitates the support that allows us to accomplish their missions, but also helps ensure that our fellow citizens understand and endorse our efforts on their behalf. I have seen the growth in the command's size, budget, and mission. That investment of resources, time, and effort is paying off, and more importantly, is helping to keep Americans safer, not only in cyberspace but in the other domains as well. I look forward to continuing the dialogue over the Command and its progress with you in this hearing today and over the months to come. And now I would be happy to address your specific questions and concerns.