STATEMENT OF

ADMIRAL MICHAEL S. ROGERS

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

SENATE COMMITTEE ON ARMED SERVICES

19 MARCH 2015

Chairman McCain, Senator Reed, and distinguished members of the Committee, thank you for the opportunity to speak to you today on behalf of the men and women of United States Cyber Command (USCYBERCOM). This is the first time I have had the honor of testifying before this Committee in a posture hearing about our Command's dedicated uniformed and civilian personnel. It gives me not only pride but great pleasure to commend their accomplishments, and I am both grateful for and humbled by the opportunity I have been given to lead them in the important work they are doing in defense of our nation.

USCYBERCOM is a subunified command of U.S. Strategic Command; we are based at Fort Meade, Maryland. Approximately 1,100 people (military, civilians, and contractors) serve at USCYBERCOM, with a Congressionally-appropriated budget for Fiscal Year 2015 of approximately $509 million for Operations and Maintenance (O&M), Research, Development, Test and Evaluation (RDT&E), and military construction (MILCON). USCYBERCOM also includes its key Service cyber components: Army Cyber Command/Second Army, Marine Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, and Air Forces Cyber/24th Air Force. Our collective missions are to direct the operation and defense of the Department of Defense's information networks while denying adversaries (when authorized) the freedom to maneuver against the United States and its allies in and through cyberspace. On a daily basis, we plan, coordinate, integrate, synchronize, and conduct activities to direct the operations and defense of specified Department of Defense information networks and the Department's critical infrastructure; and prepare to and, when directed, conduct full-spectrum military cyberspace

operations in order to enable actions in all domains, ensure U.S. and allied freedom of action in cyberspace and deny the same to our adversaries.

USCYBERCOM operates with several key mission partners. Foremost is the National Security Agency and its affiliated Central Security Service (NSA/CSS). The President's decision to maintain the "dual-hat" arrangement (under which the Commander of USCYBERCOM also serves as the Director of NSA/Chief, CSS) means the partnership of USCYBERCOM and NSA/CSS will continue to benefit our nation. NSA/CSS has unparalleled capabilities for detecting foreign threats, producing intelligence for our warfighters in all domains, analyzing cyber events, and guarding national security information systems. The best, and only, way to meet our nation's needs, to bring the military cyber force to life, to exercise good stewardship of our nation's resources, and to ensure respect for civil liberties and privacy, is to leverage the capabilities (both human and technological) that have been painstakingly built up at Fort Meade. Our nation has neither the time nor the resources to re-learn or re-create the capabilities that we tap now by working with our co-located NSA/CSS partners.

Let me also mention another key mission partner and neighbor at Fort Meade, the Defense Information Systems Agency (DISA). DISA is vital to the communications and the efficiency of the entire Department, and its people (especially those supporting the new Joint Force Headquarters-DoD Information Networks) operate in conjunction with us at USCYBERCOM on a constant basis. We also work with other federal government departments and agencies, particularly the Department of Homeland Security (DHS) and the Department of Justice and Federal Bureau of Investigation (FBI). We interact regularly with private industry and key allied nations as they seek to secure their networks, identify adversarial and criminal

actors and intentions, build resiliency for federal and critical infrastructure systems, and investigate the theft and manipulation of data.

Where We Were

This year we will mark the fifth anniversary of USCYBERCOM's activation. The Department authorized the creation of a Cyber Command in 2009, and accelerated its establishment the following year. This initiative was truly reflective of a broad consensus. The highest levels of our government saw potential adversaries militarizing cyberspace, mounting cyber espionage on a world-wide scale and using cyber capabilities to intimidate their neighbors. We also saw cyber efforts against DoD and realized the need to ensure our ability to defend its networks and command and control our own Department's forces and information systems. We in the U.S. military took the step of creating a new warfighting organization for cyberspace because we recognized that our nation's economy, infrastructure, and allies were incurring grave risks from digital disruption, and that potential adversaries were working aggressively to exploit those vulnerabilities. We saw unfriendly states, organized criminals, and even unaffiliated cyber actors stealing American intellectual property and using cyber means for coercion. USCYBERCOM was established to help stop such activities, or at least to minimize their effects on the United States and its allies.

USCYBERCOM confronted serious challenges from the outset. DoD networks had been planned and initially constructed decades earlier in an environment in which redundancy, resiliency, and defensibility were not always primary design characteristics. Operators in USCYBERCOM, not surprisingly, could not even see all of our networks, let alone monitor all the traffic coming into and out of them from the Internet. Our people were and are professionals,

so that issue was rapidly engaged, but nonetheless the sheer volume of work involved in starting a new, subunified command was substantial.

I have been at USCYBERCOM for approximately a year, and thus have had time to form some impressions of the organization and its progress. I knew when I took command that we had a sound foundation and could build upon it with confidence. The organizations had been well scoped and granted the authorities necessary to do our work. The bad news was that USCYBERCOM was built from the ground up by cutting manning to the bone, initially sacrificing vital support functions and institutional infrastructure to build mission capabilities as fast as possible. I was nonetheless pleased by the quality and dedication of the personnel across USCYBERCOM and our Service cyber components. These are professionals, in every sense of the word, and they are determined to put in place military cyber capabilities that will keep the nation safe in cyberspace. For their sake, and even more so for America's, I intend to make our organizations even stronger—and provide my successors the opportunity to do the same.

Where We Are Now

Over the last five years we have built USCYBERCOM to help defend our networks in DoD and the nation. This has not always been a straightforward process. Our Command is growing and operating at the same time, performing a multitude of tasks across a diverse and complex mission set. Of course, every command changes with events in its mission space, adjusts to evolving policies and direction, and adapts with the development of armaments and tactics. I do not want to foster the impression that we are completely unique. It is true, nonetheless, that we are constructing a new command and force while engaged on a 24-hour a day basis, every day of the year, with smart, energetic actors operating in an environment that is

highly dynamic. Some of those actors, I hasten to add, operate with no discernible legal or ethical restraints. At the same time, we are writing doctrine, training people to execute options, and keeping up with the ever-shifting topography of cyberspace. That complexity presents us—and every nation that seeks a military cyber capability—with a set of challenges that are significant.

In essence, USCYBERCOM has been "normalizing" our operations in cyberspace. We seek to afford an operational outlook and attitude to the running of the Department's roughly 7 million networked devices and 15,000 network enclaves. Collectively these represent a weapons system analogous to a carrier strike group or an aircraft strike package, through which we deliver effects. Like conventional weapons systems, our networks enable operations in other domains and distant locations, they demand constant upkeep and skillful handling, and they can be a target themselves for our adversaries. They give us the vital command and control (C2), connectivity, and intelligence for a global, 21st century military. No other nation enjoys such resources—they impart to us formidable advantages over any conceivable adversary. It is for exactly this reason that potential adversaries very much want to map, understand, exploit, and possibly disrupt our global network architecture.

In keeping with that operational mindset, we seek to impress upon commanders that cyber defense is no longer information technology (IT) it is not a mere support function that they can safely delegate to someone on their staff. Cyber is now a central part of their ability to execute their mission. It is commander's business. A successful intrusion, or severance of connectivity, can result in a direct and immediate impact to successful mission accomplishment. We have seen this happen in recent years, and though we have not yet experienced a serious,

sustained disruption to the Department's information systems, it may be only a matter of time before we face one, given the inherent vulnerability of our networks.

The fragility of that legacy architecture motivates our emphasis on deploying the Joint Information Enterprise (JIE) across DoD. We have gained significantly more visibility in our networks, but that is only a stopgap measure while the Department migrates its systems to a cloud architecture that promises to increase security and efficiency while facilitating data sharing across the enterprise. That means that the warfighter at the forward edge of battle benefits from the same data pools as our analysts, operators, and senior decisionmakers here in the United States. While the JIE is being implemented, however, our concerns about our legacy architecture collectively have spurred our formation of our new Joint Force Headquarters to defend the Department's information networks (JFHQ-DoDIN). The JFHQ-DoDIN gained then-Secretary of Defense Hagel's authorization late last year and has recently achieved initial operational capability, working at DISA under my operational control at USCYBERCOM. JFHQ-DoDIN's mission is to oversee the day-to-day operation of DoD's networks and mount an active defense of them, securing their key cyber terrain and being prepared to neutralize any adversary who manages to bypass their perimeter defenses. Placing the just-established JFHQ-DoDIN under USCYBERCOM gives us a direct lever for operating DoD's information systems in ways that make them easier to defend, and tougher for an adversary to affect. It also gets us closer to being able to manage risk on a system-wide basis across DoD, balancing warfighter needs for access to data and capabilities while maintaining the overall security of the enterprise

USCYBERCOM directs the operation and defense of Department of Defense networks, but it does much more as well, hence its formation of a Cyber Mission Force (CMF) to turn strategy and plans into operational outcomes. The Command's last two annual posture

statements have mentioned the CMF's authorization and initial steps, and I am pleased to report that the Force is very much a reality. With continued support from Congress, the Administration, and the Department, USCYBERCOM and its Service cyber components are now about halfway through the force build for the CMF. Indeed, many of its teams are generating capability today. Three years ago we lacked capacity; we had vision and expertise but were very thin on the ground. Today the new teams are actively guarding DoD networks and prepared, when appropriate and authorized, to help Combatant Commands deny freedom of maneuver to our adversaries in cyberspace. Dozens of teams are now operating; and even though many of them are still filling out their rosters and qualifying their personnel, they are proving their value daily as well as confirming the overall need for such a construct.

The work of building the CMF is not done yet. We have a target of about 6,200 personnel in 133 teams, with the majority achieving at least initial operational capability by the end of FY 2016. I have been working with the Services to accelerate the work we are doing to keep on schedule, but I can promise you that will not be easy. We are already hard pressed to find qualified personnel to man our CMF rosters, to get them cleared, and to get them trained and supported across all 133 teams. To address these gaps, I am working with our Service components, Chief, National Guard Bureau, and Reserve Chiefs to ensure we have considered a total force solution. In several areas, such as critical infrastructure, both USCYBERCOM and the Services have recognized that our Reserve Component brings us unique and valuable skills. In addition, we are charting the proper command and control relationships and structures for these teams, seeking to establish proper headquarters support for them, and giving my commanders insight into their activities so we can ensure the best possible synchronization, deconfliction, and unity of effort across the CMF. There are all sorts of good ideas for doing

this; indeed, we hear no shortage of suggestions. What I tell everyone, however, is that we have admired this issue long enough. For instance, it is time to implement and exercise measures like the objective C2 model that we agreed upon as a Department almost two years ago, even if we believe it may not end up as the permanent solution. Let us see how it works, and then change what needs to be fixed later as we gain insights from operations and the shifting threat.

Where we need help from you is with resources required to hire personnel to fill the team seats as well as necessary operational and strategic headquarters operations, intelligence, and planning staffs, facilities where we can train and employ them, and resources to properly equip them. Everyone involved knows this is a priority for the Department as well as for the Administration writ large. We also know that our Department in particular has a broad range of critical priorities, each of which competes with cyberspace for resources. This is a cold, hard reality—as is the fact that weaknesses in cyberspace have the potential to hold back our successes in every other field where the Department is engaged. Similarly, success in securing our networks and denying adversaries freedom of maneuver in cyberspace can and does bolster our DoD successes in all warfighting domains. That should factor into our resource decisions, particularly as we face the renewed possibility of sequestration—and mandatory, across-the-board eight percent budget cuts—when Fiscal Year 2016 begins a few months from now.

Let me emphasize the value of the intangibles in our work and our environment. Collectively we in USCYBERCOM have gained priceless experience in cyberspace operations, and that experience has given us something even more valuable: insight into how force is and can be employed in cyberspace. We have had the equivalent of a close-in fight with an adversary, which taught us how to maneuver and gain the initiative that means the difference between victory and defeat.

Enhancing such insight is increasingly urgent. Every conflict in the world today has a cyber dimension. Actors with modest conventional military capabilities have shown considerable capacity to harass, disrupt, and distract their adversaries through digital means. This is not, however, some on-line version of a Hobbesian state of nature; it is not a war of all against all. What we are seeing are clear patterns to cyber hostilities, and those patterns have four main trends:

- First, it has to be noted that autocratic governments in several regions view today's open Internet as a lethal threat to their regimes. For example—as President Obama noted last December—North Korea recently turned its cyber capabilities on Sony Pictures Entertainment in revenge for a forthcoming movie. The North Koreans employed unlawful cyber activities to steal and destroy data and property, to intimidate and coerce U.S.-based businesses, to threaten American citizens, and to disrupt free speech within the United States. This is unacceptable. Democracies value Internet freedom and a multi-stakeholder system of governance, in which the Internet is officially neutral with regard to free and open political speech—with clear protection for criticism and debate. We make no apologies for the fact that such neutrality is abhorrent to regimes that fear their own citizens; hence their ubiquitous and determined efforts to redefine "cybersecurity" to mean protection from "dangerous" ideas as well as from malicious activity.
- Second are the ongoing campaigns to steal intellectual property. Massive thefts of personal and institutional information and resources, by states and by criminals, have been observed over the last decade or so. Criminals are mining

personal information for use in identity theft schemes, in a sense committing fraud on an industrial scale. States have turned their much greater resources to theft as well. These intrusions and breaches have drawn comments from the highest levels of the U.S. Government. I would only add here the observation that the most worrisome of these campaigns are state-sponsored, persistent, and world-wide in scope. They are aimed at governments, non-profits, and corporations wherever they might be accruing intellectual capital that the attackers believe could be valuable, whether for re-sale or passage to competing firms and industries.

- The third form of cyber tactic we see is disruption. Once again, the actors, techniques, and targets of these incidents are numerous and varied, ranging from denial-of-service attacks, network traffic manipulation, and employment of destructive malware. We see these used all over the world, particularly in most or all of the conflicts pitting two armed adversaries against one another.
- Finally, we see states developing capabilities and attaining accesses for potential hostilities, perhaps with the idea of enhancing deterrence or as a beachhead for future cyber sabotage. Private security researchers over the last year have reported on numerous malware finds in the industrial control systems of energy sector organizations. As I suggested in my appearance before the House Permanent Select Committee on Intelligence last fall, we believe potential adversaries might be leaving cyber fingerprints on our critical infrastructure partly to convey a message that our homeland is at risk if tensions ever escalate toward military conflict.

Despite the spread of cyber attacks and conflicts around the world, we have increasing confidence in our operations-based approach. Though it is still developing and not yet fully implemented, it has nonetheless given us significant advantages in relation to potential adversaries. For instance, I can tell you in some detail how USCYBERCOM and our military partners dealt with the Heartbleed and "Shellshock vulnerabilities that emerged last year. These were unrelated but serious flaws inadvertently left in the software that millions of computers and networks in many nations depend upon; an attacker could exploit those vulnerabilities to steal data or take control of systems. Both of these security holes were discovered by responsible developers who did just what they should have done in response—they kept their findings quiet and worked with trusted colleagues to develop software patches as quickly as possible—allowing systems administrators to gain the jump on bad actors who read the same vulnerability announcements and immediately began devising ways to identify and exploit unpatched computers.

We at USCYBERCOM (and NSA/CSS) learned of Heartbleed and Shellshock at the same time that everyone else did. Our military networks are probed for vulnerabilities thousands of times every hour, so in both cases it was not long before we detected new probes checking our websites and systems for open locks, as it were, at the relevant doors and windows. By this point our mission partners had devised ways to filter such probes before they touched our systems. We were sheltered while we pushed out patches across DoD networks and monitored implementation, directing administrators to start with those systems that were most vulnerable. Very quickly we could determine and report how many systems had been remedied and how many remained at risk. Three years ago, DoD would have required many, many months to

assess the danger and formulate responses to Heartbleed and Shellshock. Thanks to the efforts we have made in recent years, our responses by contrast were comparatively quick, thorough, and effective, and in both cases they helped inform corresponding efforts on the civilian side of the federal government. We also know that other countries, including potential adversaries, struggled to cope with the Heartbleed and Shellshock vulnerabilities. In military affairs it is often relative speed and agility that can make a difference in operations; we demonstrated that in these instances, and in others that we can discuss in another setting.

This operational approach is what we need to be building in many more places. The nation's government and critical infrastructure networks are at risk as well, and we are finding that computer security is really an enterprise-wide project. To cite one example, the U.S. Government is moving toward cloud computing and mobile digital devices across the enterprise, and DoD and the Defense Industrial Base (DIB) are moving with this trend. We are working, moreover, to make our data as secure from insider threats as from external adversaries. This could eventually compel a recapitalization of government systems comparable to the shift toward desktops in the 1980s and local-area networks in the 1990s. In short, a lot of money and many people are involved at all levels. USCYBERCOM is not running this transformation, of course, but we are responsible for defending the DoD systems that will be changed by it.

Neither the U.S. Government, the states, nor the private sector can defend their information systems on their own against the most powerful cyber forces. The public and private sectors need one another's help. We saw in the recent hack of Sony Pictures Entertainment that we have to be prepared to respond to cyber attacks with concerted actions across the whole of government using our nation's unique insights and complete range of capabilities in cooperation with the private sector. This interdependence will only increase in the future. Indeed, the cyber

environment evolves rapidly—making the maturation of our capabilities and their agility in this changing mission space still more imperative for our ability to deter adversaries who might be tempted to test our resolve.

Where We Are Headed

USCYBERCOM has accomplished a great deal, but we still have a long road ahead. Cyberspace is dynamic—it changes constantly with the actions of users and the equipment and software they connect on-line. Compounding that routine volatility are two factors: the rapid evolution of the technology itself, and the changing habits and expectations of users. If current trends hold, then we can expect more nations, and even state-less groups and individuals as well, to develop and employ their own tools and cyber warfare units to cause effects in targeted networks. The cyber strife that we see now in several regions will continue and deepen in sophistication and intensity. In light of our recent experience with the destructive attacks on Sony Pictures Entertainment, we expect state and unaffiliated cyber actors to become bolder and seek more capable means to affect us and our allies. Sadly, we foresee increased tensions in cyberspace.

This is truly a period in history in which we are falling behind if we are merely holding our position in the overall movement to forge new capabilities. We in the U.S. Government and DoD must continue learning and developing new skills and techniques just to tread water, given the rapid pace of change in cyberspace. I liken our historical moment to the situation that confronted the U.S. early in the Cold War, when it became obvious that the Soviet Union and others could build hydrogen bombs and the superpower competition showed worrying signs of instability. We rapidly learned that we needed a nuclear force that was deployed across the three

legs of the riad and underpinned by robust command and control mechanisms, far-reaching intelligence, and policy structures including a declared deterrence posture. Building these nuclear forces and the policy and support structures around them took time and did not cause a nuclear war or make the world less safe. On the contrary, it made deterrence predictable, helped to lower tensions, and ultimately facilitated arms control negotiations. While the analogy to cyberspace is not exact, it seems clear that our nation must continue to commit time, effort, and resources to understanding our historical situation and building cyber military capabilities, along with the "whole-of-nation" structures and partnerships they work among. Just as we fashioned a formidable nuclear capability that served us through the Cold War and beyond, I am confident in our ability to keep pace with adversaries who are determined to control "their" corners of cyberspace, to exfiltrate our intellectual property, and to disrupt the functioning of our institutions. They are every bit as determined, creative, and persistent in these efforts as the Soviet leaders we contained during the Cold War, and unfortunately we see few hints they will act more responsibly in cyberspace. Thus we must commit to the long-term goal of building a truly open, secure cyberspace governed collaboratively by many stakeholders, while we remain prepared for crises and contingencies that can arise along the way—just as we do in every other domain.

I can assure Congress, and the American people, that we are executing and will carry out a well-conceived and systematic plan for doing that. As we train our cyber mission teams, we are inculcating a culture of respect for civil liberties and privacy while learning how to assess their readiness and establishing expectations and an institutional base that will serve to sustain this force, and even to expand it further if that someday becomes necessary. The team members we train today will furnish the leadership of the U.S. military's cyberspace organizations of the

future; they are digital natives, having come up through the ranks thinking about cyber issues. I have no doubt their perspectives will differ from our own, and that they will see solutions to problems that vex us now. Building the capabilities of USCYBERCOM and the CMF is also providing valuable lessons for the reconfiguration of DoD's networked architecture to make it more defensible. When the JIE is completely implemented a few years from now, we will have a far more secure base from which to operate in cyberspace, and all of our capabilities in the other domains will benefit as well from the massive data support they receive from a cloud architecture.

The sophistication of our defenses and operations must grow, of course, in partnership with our allies and as part of a truly whole of nation approach to the problem. Let me reiterate that there is no Department of Defense solution to our cybersecurity dilemmas. The global movement of threat activity in and through cyberspace blurs the U.S. Government's traditional understandings of how to address domestic and foreign military, criminal, and intelligence activities. This is exacerbated further by the speed with which unforeseen threats can impact U.S. interests and the fact that adversaries frequently use (wittingly or unwittingly) U.S.-based resources due to the nation's robust cyber infrastructure. This creates a circumstance in which unity of effort across the U.S. Government is required. DoD's growing capabilities and capacities need to be considered within this broader context. Any plausible solutions will involve multiple actors and stakeholders from within and across several agencies, governments, and economic sectors. Everything we do in USCYBERCOM we do in partnership with other commands, agencies, departments, industries, and countries. As we saw over the last year in our collective response to the Shellshock and Heartbleed vulnerabilities, we must all work together across the U.S. Government, with the states, industry, and allies on a constant basis to ensure we

are ready to surge for incidents and crises and thus provide the necessary assurance for inter-agency and foreign partners.

What does the future hold for USCYBERCOM specifically? I will strongly recommend to anyone who asks that we remain in the dual hat relationship under which the Commander of USCYBERCOM also serves as the Director, NSA/CSS. This is simply the right thing to do for now, as the White House reiterated in late 2013. It might not be a permanent solution, but it is a good one given where we are in this journey as it allows us to build upon the strengths of both organizations to serve our nation's defense.

Conclusion

Thank you again, Mr. Chairman and Members of the Committee, for inviting me to speak, and for all the support that you and this Committee have provided USCYBERCOM. I appreciate our continued partnership as we build our nation's defenses. Our progress has been made possible because of support from all stakeholders, in terms of resources, trust, and impetus. Cyberspace is more than a challenging environment; it is now part of virtually everything we in the U.S. military do in all domains of the battlespace and each of our lines of effort. There is hardly any meaningful distinction to be made now between events in cyberspace and events in the physical world, as they are so tightly linked. We in USCYBERCOM have strived to direct the operation and defense of DoD information systems and to protect and further the nation's interests in cyberspace. We have a great deal of work ahead of us, and thus accelerating USCYBERCOM's growth in capability will remain my focus, and be a continuing emphasis for the Department. We can all be proud of what our efforts, with your help, have accomplished in building USCYBERCOM and positioning its men and women for continued success.