STATEMENT OF

ADMIRAL MICHAEL S. ROGERS

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

16 MARCH 2016

Thank you, Chairman Wilson, Ranking Member Langevin, and Members of the Committee. I am pleased to appear before you today to talk about the opportunities and challenges facing U.S. Cyber Command (USCYBERCOM). I am honored to represent the men and women of this strong team in their work to secure Department of Defense networks and defend the interests and security of our nation, in cyberspace. I know you would be as proud of them as I am if you could see their commitment and successes on a daily basis as I do. We at USCYBERCOM welcome this opportunity to tell you how we are shifting from a focus on building the Command to an emphasis on operationalizing, sustaining, and expanding its capabilities.

By way of context, USCYBERCOM is a sub-unified command of U.S. Strategic Command (USSTRATCOM). Though USSTRATCOM is headquartered in Nebraska, we are located nearby in Maryland, where we share a corner of Fort Meade with the National Security Agency (NSA), which I also direct. Our Congressionally appropriated budget for Fiscal Year 2016 amounts to $466 million (that's $259 million for our Headquarters and $207 million for Cyber Mission Forces support). We have 963 billets for full-time employees, both military and civilian, working in USCYBERCOM's headquarters, plus another 409 contract employees. Our military contingents represent every one of the Armed Services, both active and Reserve, and they include Coast Guardsmen as well. USCYBERCOM comprises a headquarters organization and seven components: the Cyber National Mission Force, the Joint Force Headquarters-DoD Information Networks, plus joint force headquarters and growing forces at Army Cyber Command/Second Army, Marine Forces Cyberspace Command, Fleet Cyber Command/Tenth Fleet, and Air Forces Cyber/24th Air Force. Our seventh partner, though not a component, is

U.S. Coast Guard Cyber. USCYBERCOM manpower reflects a true total force effort encompassing a robust active component along with both Guard and Reserve forces being fully integrated at all echelons from the highest levels of our USCYBERCOM headquarters to our Cyber Mission Forces. Our service components are leading our integration efforts and building surge capacity, and they are doing an outstanding job. While USCYBERCOM resides with NSA, the two organizations are distinct entities with separate missions, authorities, and resource streams. Neither is an arm of the other, and both perform vital tasks on behalf of our nation.

Current Threats and Potential Threats

USCYBERCOM's mission goes well beyond defending DoD's networks and systems against cyber threats and cyber responses to those threats. Since I spoke to you last year USCYBERCOM has seen an intensification of cyberspace operations by a range of state and non-state actors. A year ago I mentioned North Korea's brazen cyber operations to impair and intimidate Sony Pictures Entertainment. We have seen no repetition of such destructive assaults against targets in the United States. On the other hand, we have seen a wide range of malicious cyber activities, aimed against American targets and victims elsewhere around the world, and thus we are by no means sanguine about the overall trends in cyberspace.

In a public forum it can be difficult to explain the nuance and depth of the threats that we at USCYBERCOM see on a daily basis. We must, however, because Congress, the federal government, industry, allies, and the general public should understand the ability and determination of malicious cyber actors. Literally every American who has connected to a network has been affected, directly or indirectly, by cyber crime. By this point millions of us have had personal information stolen, or seen our accounts or credit compromised. Even if we

have so far avoided such problems, however, we all pay higher prices for our computers and software, our Internet service, and the goods we buy as a result of cyber-enabled theft. That burden weighs on the entire economy, costing jobs and dampening growth. Just as all our citizens have benefitted from the increased productivity and speed that cyber commerce facilitates, all likewise pay the costs of cyber crime. This multi-faceted problem is the context for what follows.

At USCYBERCOM, as in the Department of Defense writ large, we focus on foreign state and non-state actors who would harm our national interests in cyberspace. Criminal activity remains the largest segment of cyber activity of concern, but nations in many ways still represent the gravest threats, as they alone can bring to bear the skills, the resources, and the patience to sustain sophisticated campaigns to penetrate and compromise some of the world's best-guarded networks. If they can gain access to those networks, moreover, they can manipulate information or software, destroy data, harm the computers that host those data, and even impair the functioning of systems that those computers control. We remain vigilant in preparing for future threats, as cyber attacks could cause catastrophic damage to portions of our power grid, communications networks, and vital services. Damaging attacks have already occurred in Europe. Just before Christmas, malicious actors launched coordinated cyber-attacks on Ukraine's power grid, causing outages and damaging electricity control systems. If directed at the critical infrastructure that supports our nation's military, cyber attacks could hamper our forces, interfering with deployments, command and control, and supply functions, in addition to the broader impact such events could have across our society.

The states that we watch most closely in cyberspace remain Russia, China, Iran, and North Korea. Russia has very capable cyber operators who can and do work with speed,

precision, and stealth. Russia is also home to a substantial segment of the world's most sophisticated cyber criminals, who have found victims all over the world. We believe there is some overlap between the state-sponsored and criminal elements in cyberspace, which is of concern because Russian actions have posed challenges to the international order.

China's leaders pledged in September 2015 to refrain from sponsoring cyber-enabled theft of trade secrets for commercial gain. Nonetheless, cyber operations from China are still targeting and exploiting U.S. government, defense industry, academic, and private computer networks. As Director of National Intelligence James Clapper testified last month, "China continues cyber espionage against the United States. Whether China's commitment of last September moderates its economic espionage remains to be seen."

Iran and North Korea represent lesser but still serious challenges to U.S. interests. Although both states have been more restrained in this last year in terms of cyber activity directed against us, they remain quite active and are steadily improving their capabilities, which often hide in the overall worldwide noise of cybercrime. Both of these nations have encouraged malicious cyber activity against the United States and their neighbors, but they currently devote the bulk of their resources and effort to working against their neighbors.

The so-called Islamic State in Iraq and the Levant (ISIL) is also a concern, though their organic capabilities to conduct malicious cyber activities so far remain limited and their main effort in cyberspace appears to be propaganda, recruiting, radicalization, and fundraising. ISIL has sought repeatedly to reach over our forces in the Middle East and carry the conflict into America itself. For instance, ISIL-affiliated cyber operators last spring posted the personal information of more than one hundred American service personnel, many of whom were here in the continental United States. Not only did the hackers for ISIL publicize the personal details on

these Americans, but ISIL also called for jihad against them, urging followers in the United States to assassinate them and their family members. While there is no direct link between this ISIL posting of personal information on service members and the recent extremist shootings in the U.S. and France, ISIL wants its followers on the Internet to take inspiration from such attacks.

In general all these various actors mount a range of cyber activities to support their interests in: a) fostering a nationalist vision of economic competition; b) intimidating émigré groups and neighbors whom they view as competitors; and c) deterring any perceived threats from other states, including ours. They steal from our corporations, and we learned last year that certain actors also stole the personal information of more than 21 million Americans that was stored in systems maintained by the Office of Personnel Management. Another group of hackers was responsible for an intrusion into an unclassified network maintained by our Joint Staff. Finally, we have seen cyber actors from more than one nation exploring the networks of our nation's critical infrastructure—and can potentially return at a time of their choosing. Collectively these actors make our government, our institutions, and our people spend far more on defense than the actors themselves spend on their efforts to penetrate our systems.

Some of these threat actors are seeking to shape us, narrowing our options in international affairs to limit our choices in the event of a crisis. As a result of these developments, we at USCYBERCOM are thinking more strategically about shifting our response planning from fighting a war to also providing decision makers with options to deter and forestall a conflict before it begins. These new options would be in addition to capabilities that help our combatant commanders succeed in their missions if and when conflict erupts and the joint forces receive an "execute order" to commence kinetic as well as cyberspace operations.

All of this work must be seen in the context of the Department's evolution of thinking toward what senior leaders call the "Third Offset" and its promise for deterring conventional as well as nuclear war. USCYBERCOM stands ready to help develop and deploy the new cyber capabilities entailed in the Third Offset, particularly hardened command and control networks and autonomous countermeasures to cyber attacks. Finally, our efforts are also proceeding in tandem with a heightened collaboration across the federal departments, agencies, and industry aimed at increasing the costs (to adversaries) of malicious cyber activities.

Progress and Prospects

Let me give you some details on how we are responding to the trends noted above. Over the last year we continued constructing USCYBERCOM while operating it at an ever-faster tempo. We have begun to transition from the "building the force" mode to a "readiness" mode. Our operations kept us busy defending the Department's networks and systems while supporting the missions of the combatant commands, especially U.S. Central Command (USCENTCOM), assisting other U.S. government entities (as authorized and upon the request of the relevant agency), and building capabilities to defend the nation against significant cyberspace attacks.

Progress in Building the Cyber Mission Force**.** To understand where we are today it is necessary to glance back at how far we have come. The Department of Defense concluded several years ago that defending the nation in cyberspace requires a military capability, operating according to traditional military principles of organization for sustained expertise and accountability at a scale that lets us perform multiple missions simultaneously. When we started to build that capability in early 2013, we had no cyber mission force, no ability to generate or train such an entity, and scant ability to respond at scale to defensive requirements or

requirements from combatant commanders. Now we have 123 teams of a target total of 133; those teams comprise 4,990 people and will build to 6,187 when we finish. In terms of progress, we have 27 teams that are fully operational capable today, and 68 that have attained initial operating capability.

The application of military capability at scale is what the Cyber Mission Force (CMF) gives us in USCYBERCOM and in the Department as a whole. Our Combat Mission Teams (CMTs) operate with the combatant commands to support their missions, while National Mission Teams (NMTs) help defend the nation's critical infrastructure from malicious cyber activity of significant consequence. We have Cyber Protection Teams (CPTs) to defend DoD Information Networks alongside local Computer Network Defense Service Providers (CNDSPs). Each of them complements the efforts of the others. I should emphasize that Cyber Mission Force teams can and do contribute to our nation's cyberspace efforts even before they reach full operational capability. Elements of teams that are still "under construction" are already assisting the combatant commands and our partner departments and agencies. Cyber Protection Teams, for instance, played important roles in defending the Joint Staff's unclassified systems after an intrusion last summer, and in remediating the vulnerabilities that the intruders had utilized.

Those Cyber Mission Force teams give USCYBERCOM the capacity to operate on a full-time, global basis on behalf of the combatant commands. The Combat Mission Teams help combatant commanders accomplish their respective missions to guard U.S. interests and project our nation's power when authorized to deter those who would threaten our security—the teams help ensure that we have the ability to enable our combatant commanders to defeat emerging threats. Such assistance occurs daily, for instance, in the fight against ISIL, as Secretary Carter recently explained in his remarks in California. Although I cannot address the particulars in this

setting, USCYBERCOM is executing orders to make it more difficult for ISIL to plan or conduct attacks against the U.S. or our allies from their bases in Iraq and Syria to keep our Service men and women safer as they conduct kinetic operations to degrade, dismantle, and ultimately destroy ISIL. The nation and every combatant commander can now call on CMF teams to bring cyberspace effects in support of their operations. Additional Combat Mission Teams under the functional commands (U.S. Strategic Command, U.S. Transportation Command, and U.S. Special Operations Command) bring still more resources to supplement those of the regional commands.

At USCYBERCOM, moreover, we control additional teams under the Cyber National Mission Force (CNMF) that can help defend America's critical infrastructure against malicious cyber activity of significant consequence. The CNMF comprise National Mission Teams, National Support Teams, and National Cyber Protection Teams to conduct full-spectrum cyberspace operations to deter, disrupt, and defeat adversary cyber actors.

DODIN Operations and Defense: At USCYBERCOM we have extended the same principles (unity of effort and command for sustained effort at scale) to the operation and defense of DoD information systems. Last year I noted that we had just established the Joint Force Headquarters (JFHQ-DoDIN) and dual-hatted the Director of the Defense Information Systems Agency to command it. Today I can proudly report that JFHQ-DoDIN has made great strides toward its goal of leading the day-to-day defense of the Department's data and networks. As a functional component command of USCYBERCOM located at DISA, JFHQ-DoDIN directs an aggressive and agile network defense. The Department of Defense as a whole is working to harden and defend its networks and systems, with USCYBERCOM providing the operational vision and directing the defense, and the DoD Chief Information Officer (CIO), working with

NSA, DISA and the military services, providing the technical standards and implementation policy. DoD CIO is measuring the cyber security status of the whole department, and for particular missions through the new CIO cybersecurity scorecard, which is provided to the Secretary each month. The Secretary recently announced another initiative as well, linked to broader Administration efforts to strengthen the nation's cybersecurity under the Cyber National Action Plan—a "bug bounty" to encourage private-sector experts (i.e., trusted hackers) to probe our systems for vulnerabilities. The goal of all of these measures is to minimize the adversary's ability to attack our systems and networks, and to detect, diagnose, contain, and eject an adversary should an attack occur.

Our operations to defend DoD networks and the nation's critical infrastructure proceed in conjunction with a host of federal, industry, and international partners (about whom I shall say more in a moment). Defending America in cyberspace is a whole-of-government, indeed a whole-of-nation, endeavor. No single agency or department has the authority, information, or wisdom to accomplish this mission alone, which is why USCYBERCOM and NSA recently updated our understandings with the Department of Homeland Security in a cyber action plan to chart our collaboration. The entire federal government, however, cannot do the job without the active participation and cooperation of the private sector. Here I compliment Congress for recently passing the Cybersecurity Information Sharing Act, which should enable industry to increase its sharing of threat information with the federal government (and vice versa) without fear of losing competitive advantage or risking additional legal liability. This is a key element in the government's efforts to improve the cybersecurity of critical infrastructure—and to frustrate adversary attempts to bend American foreign policy to their liking or even to harm Americans.

We seek to build the Command's capabilities (especially the Cyber Mission Force) with deliberate speed, and progress continues to accelerate as we learn and improve at building our teams. We remain committed to achieving full operational capability for the entire CMF by the end of FY18. Our ability to do this is shaped in no small part by consistent funding throughout the remainder of the CMF build. The key to the CMF's utility to the Department and the nation is the proficiency of its personnel. We do our best to give our people the infrastructure, tools, and support they require, but military cyber operations, despite their high degree of automation, place a premium on insight, intuition, and judgment.

Training. Cyber operators are being trained to operate mission effectiveness (for the Department and for the nation), and they must operate in a manner that respects and protects the civil liberties and privacy of American citizens. Developing a training program for cyber operators resembles the challenge that DoD faces in training pilots and aircrew to operate some of the world's most advanced aircraft, maintaining their skills on the latest aircraft systems, and sustaining their numbers to ensure a constant sufficiency of motivated and technically excellent personnel. Creating such a "pipeline" in the U.S. military's (and other countries') air components took many years, so I am hardly surprised by the persistence and complexity of the challenges that we at USCYBERCOM confront in constructing the training and personnel pipeline for the Cyber Mission Force.

Sustainment. Training the force does not automatically bring it to peak proficiency. Teams must learn to operate against live opposition, and our commanders and seniors must develop an understanding of how cyber operations unfold so they have a better idea of what to expect and what can be achieved. USCYBERCOM has been providing some insights by employing teams in the recent series of real-world operations, such as in dealing with intrusions

in DoD systems and the networks of other federal entities. Cyber Mission Teams are now regular participants in the annual exercises of the geographic and functional combatant commands, even though the demand for CMF participation outstrips our capacity to provide teams to all the exercise organizers who request them. USCYBERCOM's own annual exercises, CYBER FLAG and CYBER GUARD, offer a certain degree of realism, assembling federal, state, industry, and international partners to practice cyber defense and offense against a wily opposition force. The realism they offer is limited, however, in part because they operate on simulated networks that do not come close to approximating the scale and complexity of the Internet. We can do better, which is why the Department is building for us an advanced Persistent Training Environment to exercise our teams, and though it is not yet complete it has already been used and found very helpful.

Capabilities. Our teams require specialized tools, infrastructures, and capabilities to perform their missions. The work of improving our ability to operate in cyberspace begins in our own DoD systems; our networks are continually being probed and frequently attacked, so we are learning to combine the insights we gain from these events with our knowledge of cybersecurity to achieve situational awareness and an intuitive feel for what is coming next. In addition, USCYBERCOM has partners that possess very useful capabilities and skills, so we are constantly seeking to expand our knowledge of what is under development in the Services, national labs, agencies, as well as key foreign partners.

Innovation. Secretary Carter spoke in California recently about the importance of innovation for DoD. We heartily agree, which is why our outreach to academia and to industry is expanding as well. In the last year we established a lean but motivated "Point of Partnership" in Silicon Valley to link Command personnel to some of the most innovative minds on earth.

This new unit will help industry understand how to interact with USCYBERCOM—both how we work and where to plug in so we can work difficult, and mutual, problems together. It will also help USCYBERCOM scout technology trends, build trust, and develop mechanisms and pilot projects to facilitate the movement of the nation's cyber workforce across the public-private boundary. Our Point of Partnership is aligned and co-located with the Department's new Defense Innovation Unit-Experimental (DIUx), and we are hoping for synergy among all the DoD elements under the DIUx umbrella. Another of our efforts in this area is an ongoing set of initiatives and projects to bolster the security of hardware and software in DoD weapons systems. We are learning a great deal from this effort.

Culture. Innovation, technical upgrades, and cyber organizational changes are ongoing and necessary but by themselves are insufficient to help us fully defend our networks, systems, and information. Last September, the Department identified the need to transform DoD cybersecurity culture by improving individual performance and accountability as called for in the DoD Cyber Strategy. The Secretary and Chairman approved the DoD Cybersecurity Culture and Compliance Initiative (DC3I) to initiate a shift in the Department's cybersecurity norms. This initiative seeks to instill principles of operational excellence, personal responsibility, and individual accountability into all who provide or use cyber capability to accomplish a mission. The Department already inculcates a culture of responsibility and accountability in every DoD affiliate, both uniformed and civilian, who is authorized to handle a firearm. Our reliance on networks and data systems to accomplish our missions demands all DoD personnel understand their individual responsibilities to protect the Department of Defense Information Networks and act with similar discipline and diligence everytime they use Department systems. Instituting meaningful and lasting cultural change DoD-wide will require a long-term commitment by the

Department. USCYBERCOM was identified as the mission lead for this initiative and is working closely with Joint Staff and the Office of the Secretary of Defense to build the capacity and structure to increase cybersecurity and promote mission assurance through improved human performance in cyberspace.

DoD Cyber Strategy. Another USCYBERCOM function is to help the Department's leadership to reflect and act on the full range of issues pertaining to the cyber field Many such issues fall outside our Command's mission set, strictly speaking, but still have relevance to how the United States can and should regard cybersecurity for the nation and cyberspace capabilities as an instrument of national power. We are called upon for contributions on matters such as the implementation of the new DoD Cyber Strategy, or the defense of personally identifying information of DoD personnel and affiliates in sensitive databases, because of our level of expertise on cyber matters. Senior leaders at the Command are leading teams or serving on all of the teams charged with implementing the DoD Cyber Strategy's many initiatives, particularly the "lines of effort" regarding the training and proficiency of cyber personnel as well as the integration of cyber effects in DoD and cross-agency planning efforts. We at USCYBERCOM, of course, consult constantly our network of partners across the U.S. government to learn more. Typically a combatant command, let alone a sub-unified command, is not staffed to play such a role for the Department, but cyberspace is a dynamic environment with a host of complicated and consequential issues, and DoD has not yet had time to build up the broad and deep reserve of institutional knowledge that it possesses on other matters.

Authorities. I thank Congress and the President again for the acquisition authorities granted to USCYBERCOM in the National Defense Authorization Act for Fiscal Year 2016. Together with new manpower flexibility these presage a significant augmentation of our role of

bringing capabilities to our cyber mission teams and network defenders, as well as our ability to keep our DoD cyber workforce proficient. We are studying how best to implement that Act's provisions—such as the role of a new Command Acquisition Executive and the scope of cyber operations-peculiar equipment and capabilities—and laying the groundwork needed to put its provisions into effect after the Department drafts its implementation plan.

DoD has extensive sharing arrangements already with some of our closest allies and partners, who support our operational planning and capabilities development. These arrangements are not unlimited, but they have improved our situational awareness and helped us in the maturation of USCYBERCOM, and we have a process for managing the relationships and extending collaboration in new areas as needed. Other nations engaged in the fight against violent extremists and in planning for contingencies involving potential adversaries have also expressed their desire to partner with us. We are more limited in what we can do with them.

Let me head toward a conclusion by reflecting on how we can take advantage of the new authorities and changes discussed above in building a cyber force that is even more capable in the future. As we learn how to conduct operations to defend our nation in cyberspace, our experiences are convincing me that we across the Department may need to think again about what a 21st century military organization is. When we created USCYBERCOM we did so with the understanding that our basic principles and values remain sound; our Command was constructed to apply time-honored lessons about the need for clear and unified authorities, for consistent performance at scale, for sustainability, and for a capacity to synchronize a wide range of activities under the rule of law. I marvel at this nation's ability to assemble such resources and operate them in such a powerful manner, and I also marvel at the commitment and skill of our people—active duty and civilians alike—who answered the call to service in this new

domain. Terrorists can harm us but they have no chance of defeating such a force as long as we remain true to our national values. Nevertheless, terrorism is not the only threat we face. Other states will one day build cyber forces as capable as ours and they may attain comparable capabilities, just as the Soviets achieved rough nuclear parity with us in the Cold War. Military power in cyberspace is already something of a misnomer; cyber forces do not square off against each other and fight pitched battles like armies or fleets. Indeed, cyberspace is unlike the natural domains in many ways, and thus certain metaphors and analogies from the natural domains might just confuse matters and impair judgment. Our new cyber military force is virtually always a partner, as it rarely, if ever, acts alone. Instead, it can constitute the center of gravity for joint and combined, whole-of-government operations that defend the United States and serve the interests of the nation, and its people, and our allies. The President's *International Strategy for Cyberspace* clearly articulates our policy to exhaust other options short of military force if possible, but it also emphasizes our nation's inherent right of self-defense in cyberspace and all other domains. To exercise that right, our nation must understand how others might use force against us, and to do so we must know how force works in cyberspace, and why our nation must be able at times to depend on military capabilities that act as a nucleus of national power in this domain.

Conclusion

Thank you again, Mr. Chairman, Ranking Member Langevin, and Members of the Committee, for inviting me to speak to you today. I greatly appreciate the support that you and this Committee have provided to USCYBERCOM, and I am also grateful for the stability that you and your colleagues in Congress have provided to our resource base over the next couple

years as we complete the Cyber Mission Force build and shift our focus to sustained operations. We look to your counsel as we partner with the federal government, industry, allies, and the whole gamut of stakeholders who seek to preserve cyberspace as a free, reliable, and secure domain for exchange, commerce, culture, and progress. Our nation determined some years back that preserving freedom and security in cyberspace will inevitably mean an operational role for the U.S. military in this domain. We at USCYBERCOM strive every day to provide the sort of military capabilities and options that our leadership requires to secure and defend DoD information systems and to protect and further the nation's interests, not only in cyberspace but in all domains where our national security is challenged. I hope you will agree that our people at USCYBERCOM—while their work is not done—have already delivered handsomely on the early promise that you saw and supported. They take pride in their accomplishments, but they do not rest on them. With them, I look forward to tackling our current and future challenges together with you and our mission partners across the government. I am happy to take your questions.