STATEMENT OF

ADMIRAL MICHAEL S. ROGERS

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

SENATE COMMITTEE ON ARMED SERVICES

29 SEPTEMBER 2015

Chairman McCain, Ranking Member Reed, and distinguished members of the Committee, thank you for the opportunity to speak to you today about the implementation of our military strategy in cyberspace. It is an honor to appear today beside Director James Clapper and Deputy Secretary of Defense Robert Work as well. Let me also mention the great and justified pride I take in the privilege of speaking on behalf of the men and women of United States Cyber Command (USCYBERCOM) and the vital work they undertake to defend our nation. Their efforts, guided by the new DoD Cyber Strategy and supported by the indispensable contributions of the National Security Agency (which I also head), are improving our cyber security with the Department of Defense (DoD) and our ability to generate a greater range of options with cyber to support policy makers and operational commands. All of this helps keep our fellow citizens safe and advance our national interest overseas.

In line with the DoD Cyber Strategy, USCYBERCOM and its components perform three primary missions. First, we are responsible for securing, operating, and defending Department of Defense systems and networks, which are fundamental to the execution of all Department of Defense missions. Second, the Department of Defense and the nation rely on us to build ready cyber forces and to prepare to conduct cyber operations to deter or defeat strategic threats to the nation. Third, we work with the Combatant Commands to integrate cyber operations into broader military missions. Our military is already engaged in cyberspace. Potential adversaries scan DoD networks for vulnerabilities millions of times daily. As we have repeatedly seen, vulnerability in one place can be a weakness across an entire network and systems built as "administrative" networks are now on the front lines of our operations. This reality has serious implications for our nation's security, as well as for our military.

We are at a strategic inflection point where the great promise and opportunity offered by cyberspace innovation has also made it easier for potential adversaries to find vulnerabilities that they can use to threaten us. The DoD Cyber Strategy seeks to generate and align a multi-faceted effort within the Department against an unprecedented and growing challenge. In announcing the Strategy last April, Secretary Carter noted that threats are proliferating and diversifying. Digital tools in cyberspace give adversaries cheap and ready means of doing something that until recently only one or two states could afford to do: that is, to reach beyond the battlefield capabilities of the U.S. military. They have demonstrated the capacity to hold "at risk" our military and even civilian infrastructure. In lay terms, that means that decades of military investment is now imperiled, because as Secretary Carter says, our forces depend on the functioning of our military networks and combat systems, without which they, and we, are far less effective in all domains.

How do we know this, and what does it mean? Recent events have made this trend clear, and we know it because of our intelligence analysis. We have recently seen Russian and Chinese-sponsored intrusions in U.S. information systems – penetrations that were designed to (and in some cases did) gain persistent presence in the targeted networks. And of course, no one missed the North Korean attack on Sony Pictures Entertainment last year, when a state turned its cyber capabilities against a private U.S. corporation, stealing its intellectual property, damaging its property, disrupting its operations, invading the privacy of its employees and affiliates, and threatening its customers and suppliers. We have also observed that energy firms and public utilities in many nations (including the United States) have had their networks compromised by state cyber actors.

Secretary Carter has also noted the risk of miscalculation and escalation resulting from malicious cyber actions, and Deputy Secretary of Defense Work recently told an audience in London that conventional deterrence is eroding to a worrisome degree. Addressing that risk in the cyberspace domain is the point of the DoD Cyber Strategy – to defend, and show we can defend, and thus to preserve the effectiveness of our "traditional" instruments of national power. Let me illustrate one important way in which we are implementing this strategy, with a quick historical detour for context.

*Preparing to Respond*

Our military has found ways to adapt to new technologies, strategies, and tactics in the past. For instance, we exercised the U.S Army in Louisiana in April 1940 and learned that the sort of trench warfare that had dominated battlefields in the last World War had subsequently been overtaken by events—or more precisely, by tanks, dive bombers, and mobile infantry, all coordinated by radio. The Fall of France to the German *blitzkrieg* barely two months later showed what happened to nations that failed to heed recent advances in military art – a German force with fewer tanks and guns routed the French and British armies in just six weeks. Our War Department incorporated this lesson and returned to Louisiana in the summer of 1941 to test its new concepts. This time the U.S. Army, augmented by National Guard formations, ran two maneuvers, ultimately involving half a million troops. The first phase showed that the *blitzkrieg* could indeed be stopped, and the second showed that our Army could mount a *blitzkrieg* of its own. Those extended exercises gave us invaluable experience, prompting changes to doctrine, weapons, and concepts.

The Louisiana Maneuvers could not foreordain victory in World War II, of course, but they helped prepare our military for a new and global conflict by giving officers and soldiers the opportunity and latitude to experiment and even fail at employing new weapons, tactics, and modes of operation. Those maneuvers also drove home the point of the experimentation: to practice being agile, not just defending but being ready and able to go on the offensive and hit back, taking the fight to the opponent. That is just the sort of experimentation we must continue doing today. Then-Army Chief of Staff George C. Marshall was questioned about the expense of such large maneuvers by a Senator who also pointed out that the exercises had witnessed a lot of mistakes by the forces involved. Marshall characteristically responded respectfully but firmly: "I want the mistake [made] down in Louisiana, not in Europe." Discovery learning in the midst of real-world operations, as the British and French experienced in 1940, can be disastrous. The DoD Cyber Strategy is intended to enable us to learn in peacetime how to succeed in cyberspace operations under all conditions. Today we have "lessons learned" instead of mistakes, of course, and we are doing so in Virginia, where last summer we staged for the fourth time our large, annual exercise that we call CYBER GUARD.

We inaugurated the CYBER GUARD exercise series to test the "whole of nation" response to a major cyber incident affecting the DoDIN and U.S. critical infrastructure. USCYBERCOM offices work with experts from the Joint Staff and the joint cyber headquarters elements, Cyber Mission Force teams, U.S. Northern Command, National Guard, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), state governments, allies, and the private sector. Our defenders battle in the exercise networks against a world class "opposing force" to make this nearly three-week event as realistic as possible. The idea is to train our forces to operate as they would in an actual cyber crisis – i.e., against live

opposition and alongside the federal, state, allied, and industry partners who would also have authorities and equities in such an event. Over a thousand participants, including representatives from critical infrastructure partners and National Guard teams from 16 states, practice how to collectively protect the nation along with DoD networks. Participants from the Department of Defense practice lending appropriate support to civil authorities, and doing so on a complex exercise network that takes months to fine tune in advance of CYBER GUARD.

This latest iteration of CYBER GUARD was the largest and most realistic yet. Participants got to "maneuver" in cyberspace – seeking to see, block, and ultimately expel from the network adept opponents who had the advantages of knowing what they wanted to take (or break) and who swiftly learned their way around "our" systems. Our defenders thus experienced some of the fast-paced uncertainty of a real cyber campaign, when major decisions have to be made on the fly without the benefit of full insight into the adversary's intentions and capabilities. Players at CYBER GUARD fought through a relentless pace of events and learned that they have to trust each other for their efforts to mesh together and prove effective. To build that trust, moreover, there is no substitute for the sharing of both their information and experiences. Exercises like CYBER GUARD not only teach commanders and units how to see, block, and maneuver in cyberspace, they teach our Soldiers, Sailors, Airmen, and Marines to be teammates, both with one another and with colleagues in other parts of the federal government and private sector who we work beside to make cybersecurity effective.

CYBER GUARD showed us ways to improve our exercising of the total force and also highlighted areas where our attention is needed. This will sound familiar to many Members here assembled. I raise them to provide you with an accurate picture of the challenges in building capability and operating in the dynamic cyberspace domain.

A good analogy here is to the way our military has developed special operations forces. Our special operations forces are as good as any in the world, as we have seen over the last decade and more. Few people realize, however, what it takes for a special operations team in the field to execute a mission. They have an intensive need for critical enablers. This is the case for any maneuver element, and cyber teams are no exception. We have through CYBER GUARD and other exercises and operations a host of mission critical requirements that we are actively acquiring, building, or seeking. The Department and the government are reviewing the scope of authority for our cyber forces, including command and control relationships, manpower guidance, and development authorities to acquire the specialized tools and service we require. We are training cyber warriors and educating cyber professionals, both in the Service schoolhouses and in tailored settings. We are building out the Cyber Mission Force teams, aligning them to missions, customizing their intelligence support, assigning them to commanders, and assessing their readiness (indeed, CYBER GUARD served as a certification event for several teams; among them were teams deployed on real-world missions just weeks later). Across the cyber workforce we are setting the right mix of military and civilian personnel, and working to harmonize the several civilian hiring and career systems that take care of our people who work under parallel but not always equivalent institutional templates.

In particular, we are building a dedicated, persistent training environment, like DoD utilizes in each of the other domains. Let me explain what it is that we are doing. CYBER GUARD took place in Joint Staff facilities in Suffolk, Virginia, giving us the opportunity to practice in a controlled but more or less realistic cyber environment that we did not have to set up ourselves and then tear down after the exercise finished. Nonetheless, this was not the same as exercising in an environment specifically designed to mimic conditions on the Internet and the

real world of cyberspace, where industry partners, for instance, are independently taking steps (such as updating malware signatures and even outing cyber actors) to defend their own systems. While we defend DoD networks, of course, we are helping our federal partners to guard US Government systems as well. We need greater realism to reflect this reality in our training. With the help of the DoD Central Information Officer and others, we are now building out and testing a new exercise environment and working on interagency exercises and testing environments with partners including DHS.

Last but not least is our requirement for vital cyber infrastructure improvements to operate DoD systems safely even under attack. I have explained our need for the Unified Platform and the Joint Information Environment in previous hearings, but I will reiterate how important they are to the defense of DoD's systems and our ability to operate and deliver effects outside the United States. These improvements are the future, for they represent a revolutionary and much-needed change to the Department of Defense Information Networks (DoDIN). In addition, though information sharing alone is not a silver bullet, it is critical that the government and private sector be able to share information that will enhance the situational awareness we need to protect our nation and its interests. I am encouraged by the work that has gone into cybersecurity information sharing legislation in both the House and the Senate. But it is imperative that we finish that work and pass a cybersecurity information sharing bill as soon as possible. Cyber criminals are not waiting to steal intellectual property or financial data, so neither should Congress wait to pass this important legislation. These steps are needed to ensure that cyber remains a strategic asset, not a liability, at this strategic inflection point.

*Implementing the DoD Cyber Strategy*

Recall Secretary Carter's earlier point: if we cannot defend the infrastructure that undergirds our DoD bases and forces from foreign-based cyber threats, then our nation's military capabilities are weakened and all our instruments of national power diminished. That leaves our leaders with a need for additional options to pursue short of open hostilities, and with fewer capabilities in an actual clash of arms. This raises risk for all by inviting instability and miscalculation, as the Secretary noted.

Our nation has peer competitors in cyberspace, with other nations and groups also striving to deploy advanced cyber capabilities. They do not match our entrepreneurial élan, our manufacturing skill, or our deep investment in the theory and machinery of cyberspace. Yet they have already hinted that they hold the power to cripple our infrastructure and set back our standard of living if they choose. They know, of course, that we can hit back, and that potentially devastating cyberattacks against U.S. interests would ripple across the global economy. But they could well count on deterring us in a regional crisis, making our leaders hesitate and muffle American responses to aggression overseas. Such delays could give them time to continue their encroachments, attain their objectives, and consolidate their gains.

We need to understand the systemic-level implications of what is happening. We are, in effect, being strategically shaped by potential adversaries. They also feel entitled to turn the resources of their states against private business, research labs, academic institutions, and even individual citizens in the West to steal the fruits of our creativity, or negatively impact the enjoyment of human rights and fundamental freedoms, including the freedom of expression.

This context adds the sense of urgency we feel at USCYBERCOM and across the Department of Defense. How do we prevent potential adversaries from shaping us and deterring our defense of America's interests and allies? We know that the DoD Cyber Strategy gained the attention of countries overseas – this enhances deterrence right here. But that is only one step of many. We need to take several more steps as we implement that Strategy.

First, we have to continue the whole-of-government coordination that makes our words and actions far more meaningful to potential adversaries. As Secretary Carter stated in announcing the DoD Cyber Strategy, we need synchronized inter-agency measures to bring all the powers and authorities of the U.S. government to bear on malicious cyber actors. Individual sanctions, indictments and other steps are effective tools, but they might not be sufficient by themselves because potential adversaries believe they have too much to gain from continued cyber-enabled theft of our intellectual property and continued intimidation of their neighbors through cyberspace (among other mechanisms, of course).

Second, we must deepen our partnerships. Organizations across the U.S. Government must create consistent, complementary approaches for operating with private sector and international partners—leveraging the comparative advantages of civilian, homeland security, law enforcement, intelligence community, and military entities. Many departments and agencies share the authorities and responsibilities to guard critical infrastructure in the United States, and we look to DHS' Industrial Control Systems Computer Emergency Readiness Team (ICS-CERT) for information-sharing, incident response and mitigation. We as a nation need to enhance governing policies and legal frameworks to enable a robust defense of the defense industrial base and other sectors of our critical infrastructure. This could include efforts across

the Government to identify and manage risks to our critical infrastructure and key resources in the near term, while transitioning from a reactive to a deterrent posture over the long term.

Finally, we must forge a consensus on when we can and should respond to cyber activity directed against the United States. Such a consensus should clarify the proper role of the military in a whole-of-nation approach to improving our security in the cyberspace domain. The President has stated that we reserve the right to respond with all instruments of national power to cyberattacks against our critical infrastructure. Here is where we particularly need to build trust in the ability of the U.S. Government—on the civilian and military sides—to exercise its powers and capabilities responsibly to defend the nation, consistent with international law and norms. I see my job in this entailing an effort to better explain certain concepts like "offensive cyber operations" and the Cyber Mission Force. I welcome your ideas on this.

*Conclusion*

Thank you again, Mr. Chairman and Members of the Committee, for inviting me to speak on behalf of USCYBERCOM about the vital topic of cyberspace strategy. Our Command is helping the Department and the federal government mitigate risk while unleashing the promise and opportunity inherent in cyberspace in ways consistent with our values as a nation. As you can tell from the foregoing, I take pride in the accomplishments of our men and women. I know they will give their all in executing our Command's missions and in forging cyber forces that offer our nation's leaders a full suite of options in cyberspace and beyond. With their great efforts and your continued support, I know we can be positioned for success, despite the seriousness of the current situation. There is no single technical or engineering fix alone that is

going to solve these challenges, but instead we will require a great deal of the fortitude, creativity, and determination that we Americans have repeatedly shown we can muster. I look forward to your questions and to advancing this important dialogue.