STATEMENT OF

GENERAL KEITH B. ALEXANDER

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

HOUSE COMMITTEE ON ARMED SERVICES

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

16 MARCH 2011

Chairman Thornberry, Ranking Member Langevin, and distinguished members of the Subcommittee on Emerging Threats and Capabilities, thank you for inviting me today to represent the extraordinary men and women of the United States Cyber Command and deliver the Command's posture statement. I want to begin my remarks by thanking you and your colleagues in Congress for helping us to build this Command and assisting its efforts to accomplish its mission. Cybersecurity is vital to our nation—perhaps now more than ever—and part of our task is ensuring that our nation understands what it is that you, the White House, and the Department of Defense have charged us to do and why it is so important that we do it well. I look upon these remarks before you as an invitation for dialogue about the roles, missions, and capabilities of Cyber Command, and I am eager to hear your views on how we are doing and where we should be going.

Before proceeding, I also wish to thank the great leaders and partners we have had in building the capabilities of US Cyber Command since its creation last year. Secretary of Defense Gates, Deputy Secretary Lynn, Chairman Mullen, and Vice Chairman Cartwright have been particularly supportive, as has General Kehler, the new Commander of US Strategic Command. Our Combatant Commands, moreover, have been appreciative of our initial steps, applauding initiatives to pioneer new ways of presenting cyber capabilities to the Joint force. We also owe a great deal of gratitude to the dedicated professionals of the National Security Agency / Central Security Service (NSA/CSS) whom it is also my honor to lead. Their contributions are significant, along with those of the Defense Information Systems Agency and our many other partners inside and outside of the U.S. government. There are many others I

could name here, but in the interest of brevity and to leave more time for a dialogue with you, I shall forbear.

If you will, allow me to brief you on what has been happening at US Cyber Command and where we are trying to go. Constructing a new Command while conducting operations is quite a challenge, especially in a time of rapid technological and policy changes, but we have produced results that have made our nation stronger and more secure. Let me emphasize this point: Cyber Command has already returned cybersecurity dividends on the investments of time and resources dedicated to its creation. We are making progress, and with your help, we will surmount the issues that remain for us as we accomplish our mission.

The Road to Full Operational Capability

US Cyber Command achieved full operational capability (FOC) on 31 October 2010 as a subunified command under US Strategic Command (USSTRATCOM). The road to FOC culminated roughly according to the timetable prescribed by the Secretary of Defense when he directed the establishment of the Command back in June 2009. Initial operational capability (IOC) was originally projected to have been reached that October, but that date slipped to May 2010, when my nomination to serve as its first Commander was confirmed by the Senate. We put the months between October 2009 and May 2010 to good use, however, building a consolidated staff to merge the two legacy organizations, Joint Functional Component Command for Network Warfare (JFCC-NW) and Joint Task Force for Global Network Operations (JTF-

GNO), which together became Cyber Command. We also outlined the tasks needed to move us to FOC once the clock started running. Though the interval between initial capability in May and attaining full operational capability in October was only five months instead of the planned twelve, we were able to accomplish a number of key activities. Moreover, we did all this while accelerating the tempo of daily operations that had been established by JTF-GNO and JFCC-NW.

Despite the compressed schedule, the consolidated staff at the nascent Cyber Command was able to accomplish a great deal by last October. We established a Joint Operations Center, transferred operational control of the JTF-GNO mission set to Ft. Meade, Maryland, and stood down JTF-GNO's 24/7 watch center in Arlington, Virginia, which helped USSTRATCOM disestablish JFCC-NW and JTF-GNO. The latter task took a considerable amount of planning and careful orchestration because JTF-GNO's activities and workforce had to be transitioned from Northern Virginia to Ft. Meade while ensuring the daily functioning of the Department of Defense's networks were unimpaired. We established effective operational command and control processes for the consolidated mission sets. A Joint Intelligence Operations Center was established. Our Service cyber components were formally assigned to USSTRATCOM, and we continued building relationships with key partners. We embedded liaison officers at the Combatant Commands and set conditions to expand their presence to larger Cyber Support Elements. We deployed expeditionary teams to support operations in Iraq and Afghanistan. We also made progress in our support of operational planning by the Combatant Commanders and in building processes for them to issue requirements for cyber support. We accomplished all of this

without negative mission impact, keeping the Department's operations secure while making the transition transparent to users of its information systems.

Our overall success during this critical phase was not without challenges, and there remain some important issues yet to be resolved even after Cyber Command's attainment of FOC. The Department has a shortfall of cyber force capacity to plan, operate, and defend its networks and ensure freedom of action and maneuver for our nation in cyberspace. Additionally, we are still discussing across the Administration how to best defend against a "Cyber 9/11" that affects our critical infrastructure and beyond. Finally, we have only begun our effort to take advantage of significant efficiencies in designing and managing our information technology architecture.

US Cyber Command continues to build synergy with NSA/CSS to take advantage of NSA/CSS's infrastructure and expertise, which remain crucial to our progress. Our co-location allows the government to maximize our collective talent and capabilities. The Command's Fiscal Year 2012 budget is projected to be $159 million, and our workforce at that point is slated to be 464 military personnel and 467 civilians for a total of 931 employees plus focused contract support. The overall mission of this team is to plan, coordinate, integrate, synchronize, and conduct activities to direct the operations and defense of specified Department of Defense information networks; and prepare to, and, when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US and Allied freedom of action in cyberspace, and deny the same to our adversaries. Let me turn now to the environment in which we are executing that mission.

Current Perspectives

When I spoke before the full committee last fall, a month before the declaration of full operational capability, I offered my explanation of cyberspace, noting the importance to our nation of maintaining our freedom of action to this new, unique, man-made domain and preserving our security in it. I also spoke of the challenges that we face in doing so. Yours is one subcommittee that needs no reiteration of these points, and so I shall move on directly to more recent developments and our evolving perspectives on how to deal with them.

The cyber threat continues to mature, posing dangers that far exceed the 2008 breach of our classified systems we discussed last fall. Our leaders from President Obama on down have emphasized this point, and for good reason. Our nation now depends on access to cyberspace and the data and capabilities residing there; we are collectively vulnerable to an array of threats ranging from network instability to criminal and terrorist activities to state-sponsored capabilities and actions that are progressing from exploitation to disruption to destruction. While I hasten to say that we have not suffered disastrous or irreparable harm in cyberspace from any of these risk categories, we must be prepared to counter this evolving threat.

Both external actors and insider threats pose significant challenges to our cybersecurity.

No state actor, of course, has admitted to launching disruptive cyber attacks on another state. Yet incidents have occurred that look a great deal like such attacks. The cyber assaults on

Estonia in 2007 spurred us and our NATO allies to deliberate regarding what in cyberspace would constitute an "armed attack" on an alliance member that would trigger the North Atlantic Treaty's provisions on collective defense. The following year, the invasion of Georgia coincided with precisely targeted cyber attacks, marking one of the first times we have seen such "cyber supporting fires." The coincidence was so perfect that independent observers concluded there was no coincidence—that the hackers who temporarily crippled the Georgian government's response and communications with the outside world had practiced their assaults and responded to official cues when they mounted them for real.

We have recently seen Internet access manipulated or curtailed by governments to suppress and disrupt even peaceful protests by their own citizens. In addition, we believe that state actors have developed cyber weapons to cripple infrastructure targets in ways tantamount to kinetic assaults; some of these weapons could potentially destroy hardware as well as data and software. The possibilities for destructive cyber effects, having long been mostly theoretical, are now real and increasingly available; we must worry not just about their intentional use, but also about their accidental release. Segments of our nation's critical infrastructure are not prepared to handle this kind of threat.

Bear in mind that we also watch with concern the growing capabilities of non-state actors. The threats we see here are asymmetric, meaning that comparatively new or lesser players can cause effects commensurate with state-sponsored actions; a small and inexpensive operation can divert government resources for spotting and diagnosing a problem, neutralizing the malware employed, patching the exploited vulnerability, and recovering from the

institutional (and personal) damage it caused. Although individuals with computer skills have independently shown that such attacks can be launched by even a lone actor with a laptop and a motive, we are chiefly focused on terrorists and well-organized cyber criminals. The former continue to grow more proficient in using the Internet as a medium for recruitment, coordination, and other activities, and they are becoming ever-more sophisticated in doing so. Cyber criminals are more interested in the theft and exploitation of sensitive data that can bring them a profit, either directly through fraud or identity theft, or indirectly through the pirating of intellectual capital. Indeed, observers such as Senator Sheldon Whitehouse and a bipartisan team of colleagues last summer called this as "the biggest transfer of wealth through theft and piracy in the history of mankind"—a transfer that has significantly lowered the cost for potential adversaries to close and counter our technological lead. Such activity is crime, of course, and belongs more properly in law enforcement than military channels, but when a prime target of such crime is our defense industrial base, we in the Department of Defense have a role to play in the response. We also find that state actors and terrorists can exploit the breaches and tools made by criminals, much as a dangerous pathogen opportunistically employs a disease vector to enter a host. Indeed, sometimes the state and non-state actors collaborate on matters of mutual interest.

Various threats that emanate from poor cyber hygiene, inadvertent misuse, and malicious actions also create significant security challenges. After all, even the most astute malicious cyber actors—those who can break into almost any network that they really try to penetrate—are usually searching for targets of opportunity. They search for easy vulnerabilities in our systems security and then exploit them. I am very concerned by the ways in which neglect makes us vulnerable. The unapplied software patches, the firewalls left unattended, and the anti-virus

suites that never get updated even in the US military cause us more trouble than I like to admit, especially when a risk to one is a risk shared by all. Now multiply those problems across the government and the private sector, and realize that we have networked our vulnerabilities while segmenting our defenses among the .mil, .gov, .com, and .edu Internet domains. Each domain (and often each system) has been left to fend for itself against cyber actors who care little for legal distinctions and organizational boundaries. And finally there is the insider threat; I am sure I need not remind anyone that some of the largest security breachs in history have originated from insider threats.

The recent creation of Cyber Command has garnered a great deal of interest from foreign militaries and the governments that oversee them. We see frequent media reports on nations contemplating the creation of their own "cyber commands." I see this as a sign not necessarily of a "militarization" of cyberspace but rather a reflection of the level of the concern with which civilian and military leaders around the world are viewing current problems. Many such steps are essentially defensive, and if so many nations are interested in improving their defenses, they are probably even more willing to talk about ways they can reduce common threats. There is a rough, *de facto* deterrence at the strategic level of cyberspace. Although no one knows how a cyber war would play out, even the most capable state actors seem to recognize that it is in no one's interest to find out the hard way. I am convinced this concern has led to a certain degree of restraint by states that we deem capable of causing very serious cyber effects. Lest optimism obscure real threats, however, I must add that we have no certain capability to restrain the behavior of radical, non-state extremists.

In sum, our adversaries in cyberspace are highly capable. Our defenses—across dot-mil and the defense industrial base (DIB)—are not. Our economy, our society, and all of us have become directly or indirectly dependent on access to and freedom of movement in cyberspace—and indeed our military is equally dependent on such access—and thus we cannot be content with a situation in which we are sometimes our own worst enemies.

Next I want to tell you about some of the things we are doing and planning at Cyber Command to ensure that the Department of Defense has done all it can to defend and deter determined adversaries, mitigate dangerous threats, and address nagging vulnerabilities, so that even our most capable opponents will know that interfering with our nation's equities in cyberspace is a losing proposition.

Working toward the Future

As you can gather from the foregoing discussion, US Cyber Command faces serious challenges as it comes together to do urgently needed work in cyberspace. Our establishment reflects the department's need to manage cyber risk, secure freedom of action, and ensure the development of integrated capabilities. Our intent is to overcome the challenges we face through the concerted efforts of implementing The National Military Strategy of the United States of America 2011. We will pursue resolution of the capacity, resources, and information technology efficiencies issues we face through the five strategic initiatives of the department's strategy. We intend to:

- Treat cyberspace as a domain for the purposes of organizing, training, and equipping, so that DoD can take full advantage of cyberspace's potential in military, intelligence, and business operations
- Employ new defense operating concepts, including active cyber defenses, such as screening traffic, to protect DoD networks and systems
- Partner closely with other U.S. government departments and agencies and the private sector to enable a whole-of-government strategy and an integrated national approach to cyber security
- Build robust relationships with U.S. allies and international partners to enable information sharing and strengthen collective cyber security.
- Leverage the Nation's ingenuity by recruiting and retaining an exceptional cyber workforce and to enable rapid technological innovation.

In this context, let me show you the reasoning behind our planning and activities, and give you a sense of where we might need assistance in reaching our goals. The best way to organize this discussion is by our Command's mission areas. As noted earlier, we were established to operate and defend Department of Defense networks. When I see you again a year from now, I intend to report that we are executing that mission and achieving greater security for our networks.

Our first duty is to ensure that Department of Defense networks are secure. Securing these networks is crucial to protecting our data, to our warfighting potential, and ultimately to the defense of our nation. Until recently we all viewed our networks as a great force multiplier—the magic that let us put ordnance on target and dispatch planes, troops, and ships to where they were needed, when they had to be there. Today, however, we understand that those networks

represent a serious vulnerability, and we dread the thought of someone getting inside to bring them down or, perhaps even worse, to make a few subtle changes to the integrity of our data that bring all our military operations to a halt. Without fast, assured, and safe data flows we will not be able to fight our adversaries the way we as Americans think they should be fought. We are not necessarily close to losing that edge, but potential adversaries understand where it lies, and are certainly contemplating ways of blunting it in any future conflict.

Cyber Command is working to preserve that information advantage in many ways. We are directing the operations of the Department's information networks, which knit together seven million computing devices spread across fifteen thousand networks. The recent move of the Defense Information Systems Agency to a new facility near us on Fort Meade has enabled even greater collaboration between our two organizations. Cyber Command and DISA collaborate on a daily basis to monitor the functioning of the Department's information networks. That work includes the maintenance of sensors to detect and block adversary activity in those networks, the inspection of security settings and practices, and the investigation of real and suspected incidents. Together we are making progress in all of these areas, and I am more comfortable today than I was twelve months ago in our ability to stop intrusions and adapt to changing adversarial practices almost as fast as they evolve. The new sensor capabilities we are deploying and the aggressive inspection regime now coming together will improve our situation even more over the year to come.

We also plan, in partnership with NSA, the defense of specified Department of Defense information systems, knowing that we have to stay ahead of the cyber threat in technological

terms. Here US Cyber Command and our partners in the Department are working on ways of shifting to a different and more defensible architecture for providing information services to users. A year from now we should be well on our way to having a hardened architecture proven and in place, which provides a new level of cyber security. The idea is to reduce vulnerabilities inherent in the current architecture and to exploit the advantages of "cloud" computing and thin-client networks, moving the programs and the data that users need away from the thousands of desktops we now use—each of which has to be individually secured for just one of our three major architectures (NIPRNet, SIPRNet, and JWICS)—up to a centralized configuration that will give us wider availability of applications and data combined with tighter control over accesses and vulnerabilities and more timely mitigation of the latter. Moving to a cloud architecture has the advantages of producing economies of scale and reducing the Department's information technology costs. This architecture would seem at first glance to be vulnerable to insider threats—indeed, no system that human beings use can be made immune to abuse—but we are convinced the controls and tools that will be built into the cloud will ensure that people cannot see any data beyond what they need for their jobs and will be swiftly identified if they make unauthorized attempts to access data.

A year from now I look forward to telling you that we have "operationalized" our Department's networks. We will, of course, continue to do this with full regard for and protection of the privacy and civil liberties of US persons as well as in compliance with all applicable laws and regulations. The idea is to transform the Department of Defense's information systems from something to be passively guarded into a suite of capabilities that offer our commanders and senior leaders opportunities to adjust our defenses. If people who seek to

harm us in cyberspace learn that doing so is costly and difficult, we believe we will see their patterns of behavior change. The technology is ready and I encourage a conversation on the privacy and civil liberties impact of such technology and how to adjust laws and policies to allow the use of this technology for cyber defense.

Our Command's mission document states that we coordinate, integrate, and synchronize activities to direct the operations and defense of the Department of Defense's networks. In practice, that means we spend a great deal of time talking with leaders and experts in the Department, the U.S. Government, private industry, and other nations as well. This effort begins, of course, with US Cyber Command Service cyber components that provide the forces that implement our plans and execute our directives (they are the Army Cyber Command, Marine Corps Forces Cyber Command, Fleet Cyber Command, and Air Force Cyber Command). We are still maturing the way in which we and they will interact to support and be supported by the geographic combatant commands in various situations. Our mission depends as well on the work of the National Security Agency, which provides the expertise and intelligence that are indispensable to understanding what is happening in cyberspace. We are constantly engaged with DISA as well, and our relationship with them will likely change substantially and become even closer in the near future. In addition, since I spoke to you last fall we have strengthened our strategic partnership with the Department of Homeland Security in accord with the recent agreement concluded by Secretaries Gates and Napolitano. A senior DHS official now works at NSA with us and attends many of our leadership meetings, and several government agencies are also represented 24 hours a day in our Joint Operations Center. These measures, along with complementary measures at Department of Homeland Security and other partners, should

provide a whole-of-government awareness of what everyone is seeing so that we can plan for and execute authorized and coordinated joint actions in the event of an emergency. Finally, we are active players in the Department of Defense's productive discussions between government and industry over how to share information regarding common threats and potential ways of mitigating them. The vast majority of our military's information packets ride on commercial infrastructure, and thus we need to develop shared insights into those dependencies for mission assurance purposes.

The second part of our mission at Cyber Command is to be prepared to conduct full spectrum military cyberspace operations in order to enable actions in all domains. As I noted above, states and non-state actors have already experimented with ways of harassing or attacking rival governments, whether to make a strategic point or in conjunction with kinetic attacks. Our military and our nation would be unwise to assume that we have seen the last such attacks. We are prepared, when directed and in full compliance with applicable laws, including the Constitution, federal statutes, and the Law of Armed Conflict, to respond when we or our allies are threatened or subjected to the use of force in the cyberspace. The President has emphasized that our digital infrastructure is a strategic national asset and insisted that preparing our government for the task of protecting strategic national assets in cyberspace is a national security priority. Our efforts to do this are designed to achieve two goals:

- First, we protect US and allied freedom of action in cyberspace. It is no longer possible to conceive of our nation functioning properly or even defending itself without the ability to create, transmit, and secure masses of digitized data. Making our access to cyberspace

impossible or even problematic would represent a strategic threat to America's vital interests—one that our Command has been established and tasked to prevent with respect to DoD's operations in the cyberspace. Furthermore, our cybersecurity is inextricably linked with that of our allies, and our interests in cyberspace often coincide with those of other states with whom we have less-formal ties. The lack of geographic borders in cyberspace means that a threat to one can be a threat to all, which gives us a real incentive to share situational awareness and best practices that help to protect our military, government, and private networks and data.

- Second, when directed, we need to deny freedom of action in cyberspace for our adversaries pursuant to appropriate authorization and consistent with applicable law. Working with the Executive Office of the President and other U.S. government departments and agencies, US Cyber Command stands ready to support the development of all necessary policies for cyberspace operations. As with all activities that DOD pursues, operations are only executed with a clear mission and under clear authorities, and they are governed by all applicable laws, including the Law of Armed Conflict. We cannot afford to allow cyberspace to be a sanctuary where real and potential adversaries can marshal forces and capabilities to use against us and our allies. This is not a hypothetical danger; we have seen adversaries use the Internet to harm US forces and coalition partners. At Cyber Command much of our focus is on helping our troops in the field limit their vulnerabilities in and from cyberspace. This effort reflects the likelihood that; henceforth all conflicts will have some cyber aspect, and our efforts to understand this development will be crucial to the future security of the United States. DoD is

collaborating with the Executive Office of the President and other Departments and Agencies to resolve outstanding policy and authority questions.

We are making progress executing these missions, but I also want to share with you one of my chief concerns. The importance of the cyber mission is something that our Department and its constituent Armed Services did not anticipate or build forces to address. As we improve our common operating picture and our intelligence to understand what is happening, as well as our operations to create effects, we are finding that we do not have the capacity to do everything we need to accomplish. To put it bluntly, we are very thin, and a crisis would quickly stress our cyber forces. The problem has two facets—there are too few trained Service personnel out there in the first place, and also the Services need to hold on to as many of them as they can. Thus in both of the mission areas above, the biggest issue I see is the need for collaborative force development (including joint standards, recruitment, training, deployment, sustainment, and retention).

We at Cyber Command also need to grow the authorities we work under. A year from now we hope to have robust authorities for key enablers like budgeting, training, and career development, as well as for the swift acquisition and testing enabling technologies. We will also build our collaboration with national and Service research and development laboratories. All of these steps will, I believe, make us much better postured to accomplish the mission that our nation has entrusted to us.

Conclusion

I thank you again for calling me before you today and allowing me the opportunity to submit this posture statement on behalf of US Cyber Command. The Department of Defense took an important step for our nation in creating this Command and declaring it to be in full operational capability status last fall. I have described our philosophy of actively managing the Department's information networks—not just to defend them, but to use them as a tool to assist our warfighters, planners, and commanders by preserving their freedom of action—and also to be as ready to use our own capabilities to disrupt any adversarial use of cyberspace against US interests. If I may, I'd like to reiterate our intention to:

- Increase the capacity of the cyber workforce;
- Implement and exploit, in a strengthened partnership with NSA, the transformation of the Department's networks;
- Work with the Combatant Commands to synchronize processes and planning to deliver the joint effects they require;
- Support DOD, DHS, and other Government partners in the extension of cyber defense capabilities across the U.S. Government's network and,
- With DHS, increase our government's dialogue with private partners on the protection of our nation's critical infrastructure.

We in Cyber Command operate with respect for civil liberties and in compliance with the laws governing the privacy of our fellow Americans, in accord with the directives of the national command authority, and, in conjunction with our mission partners in the Departments of Defense and Homeland Security, law enforcement, the intelligence community, industry, and academia. We do not see the security of our nation and the protection of civil liberties and privacy as a balance; rather, we believe we can and must defend both. I thank you for your help in this endeavor, and I am confident that together we will succeed. And now I look forward to your questions.