NOT FOR DISTRIBUTION UNTIL RELEASED BY THE

HOUSE COMMITTEE ON ARMED SERVICES

STATEMENT OF

GENERAL KEITH B. ALEXANDER

COMMANDER

UNITED STATES CYBER COMMAND

BEFORE THE

HOUSE COMMITTEE ON ARMED SERVICES

23 SEPTEMBER 2010

NOT FOR DISTRIBUTION UNTIL RELEASED BY THE

HOUSE COMMITTEE ON ARMED SERVICES

Chairman Skelton, Ranking Member McKeon, and distinguished members of the Committee on Armed Services, thank you for inviting me today to represent the extraordinary men and women of the new United States Cyber Command and deliver the Command's first posture statement. Indeed, I want to begin my remarks by thanking you and your colleagues in Congress again for helping to make this Command a reality as we move forward to address threats and concerns to our nation. We have a big job in front of us, not only in terms of accomplishing our mission but also in terms of ensuring that our nation understands just what it is that you, and the White House, and the Department of Defense have charged us to do. I want to take this opportunity to explain how we look at that vital job and how we are organizing to meet its challenges. I see these remarks as an invitation to a dialogue about the roles, missions, and capabilities of the Department of Defense in cyberspace, and I am eager to hear your views on how we should be proceeding.

Before going any further, however, I also need to thank the great partners we have had, both in the effort to establish US Cyber Command and in our work of building its capabilities. Cyber Command and its early progress simply would not have been possible without the sustained leadership of President Obama, Secretary of Defense Robert Gates, Deputy Secretary of Defense William Lynn, General Kevin Chilton, and many others, including Secretary of Homeland Security Janet Napolitano, Director of National Intelligence James Clapper, Chairman Michael Mullen, Vice Chairman James Cartwright, General David Petraeus, Admiral Robert Willard, General Duncan McNabb, Admiral James Stavridis, Deputy Director Chris Inglis, Acting Assistant Secretary Cheryl Roby, and Lieutenant General Carroll Pollett. We also owe our gratitude to the White House, US Strategic Command, the National Security Agency (NSA), the Defense Information Systems Agency (DISA), and our partners in the intelligence community, law enforcement, homeland security, and industry. That list, while large, is not comprehensive, as there were significant contributions from too many others to name everyone.

My aim is to describe what is happening at US Cyber Command. I shall provide an overview of where we think we are—both in building the new Command and in the larger context of the global changes that have brought about the need to create a cyber command—and then tell you how we plan to move forward in accomplishing the mission assigned to us.

Creating a New Command

US Cyber Command is a sub-unified command under US Strategic Command. We are combining two entities from US Strategic Command: the Joint Functional Component Command for Network Warfare and the Joint Task Force-Global Network Operations, along with a consolidated staff that temporarily bridged these two legacy organizations. When the Cyber Command Staff reaches full operational capacity it should have around 1100 personnel**,** mostly military but with some civilian officials, and focused, on-site contract support. In a sense we in the Command are swapping out the engine of a race car at high speed; creating an enhanced cyberspace capability while conducting cyberspace operations in support of the Department of Defense and other departments and agencies.

Based on the Secretary of Defense's announced efficiency initiative, we are examining how we support this important program and how it might affect us at US Cyber Command. It is possible that resources saved from the stand-down of the Office of the Assistant Secretary of Defense for Networks and Information Integration will boost US Cyber Command. The Command's requirements, along with those of the rest of the Department, are being reviewed now and will be addressed in the Fiscal Year 2012 budget.

As your subcommittee on Terrorism and Unconventional Threats and Capabilities will hear this afternoon, the Service cyber components assist us in Cyber Command. Indeed, they are the organizations and the people who do much of the work of the Department of Defense in cyberspace. What we do as US Cyber Commend in many cases will actually get done through Army Forces Cyber Command, the Navy's Fleet Cyber Command, the 24th Air Force, and Marine Forces Cyber Command. We are working closely with the Joint Staff, Combatant Commands and the Services to determine the optimal way US Cyber Command will exercise command and control over the constituent units associated with these components. I look forward to reporting to you on this topic in the near future.

The National Security Agency (NSA) contributes essential expertise for our activities, both in supporting the accomplishment of our mission and in terms of day-to-day support. As you know, I also serve as the Director of NSA and the Chief of the Central Security Service (CSS). NSA/CSS's infrastructure and expertise have been crucial to our progress so far. The core of what NSA/CSS does will not change as Cyber Command grows. Those organizations will continue to lead the US cryptologic community on the signals intelligence and information assurance fronts. The professionals at NSA/CSS have a history of success and expertise, and as a customer, Cyber Command will leverage those capabilities. In our work at both NSA/CSS and Cyber Command we see how much the world is becoming networked and inter-connected. NSA/CSS more and more finds itself conducting its traditional signals intelligence and information assurance missions in the cyber domain. As Cyber Command stands up, it is vital to develop synergy with NSA/CSS in order to take advantage of NSA/CSS's longstanding competence and its outstanding capabilities—especially its deep commitment to supporting ongoing military operations and its mature processes for producing intelligence while respecting the privacy and civil liberties of US persons. Indeed, those achievements have already allowed Cyber Command to take prudent risk by focusing our efforts on building our mission capabilities now, in the light of protecting privacy and civil liberties, while letting our support functions follow. Having Cyber Command co-located with NSA/CSS will benefit the Agency now and in the long run; enabling us to build a vital partnership, leveraging intelligence to support defense and helping us conduct our respective missions in concert – while ensuring that we respect and honor our commitment to the law and the privacy of our fellow citizens.

Last, but by no means least, we also receive support from the Defense Information Systems Agency, which plans, acquires, and maintains the communications backbone that our Department of Defense's data ride on. DISA has run the Department's networks for decades, and it continues to play a significant role as we move forward. Its impending move to Fort Meade will allow for the development of closer working relationships between DISA, NSA/CSS, and Cyber Command – and it will help us ensure that future government telecommunications infrastructure design is done in close coordination with still more organizations that are well-versed in network security.

The Strategic Environment in Cyberspace

Deputy Secretary William Lynn noted recently that the key to Cyber Command is its "linking of intelligence, offense, and defense under one roof." How will that actually work? Before explaining our plans for US Cyber Command, it might be helpful to describe what we might call our "common operating picture." This entails an explanation of the environment in which our Command functions and how that is changing, and a description of the actors who inhabit it with us—some of whom give us increasing grounds for concern.

Cyber Command has a unique "area of responsibility" that literally changes its characteristics and its dimensions continuously. For instance, since 2000, world Internet usage has increased by 400 percent. In 2009 there were more than 1.8 billion Internet users, and 4.6 billion cellular subscribers; together they sent roughly 90 trillion e-mails. Cyberspace in that sense is "larger" than ever. And yet, at the same time, bandwidth is broader and search engines are more powerful than ever, and so in a different sense cyberspace has become "smaller," with more and more people able to interact with each other in real-time.

The US military began thinking formally about cyber matters almost twenty years ago. Cyberspace can be tough to understand at first glance—what does it mean when machines talk to other machines, and how does that affect us here in the real world? The Joint Chiefs of Staff deemed cyberspace a "domain" within the last decade, but what does that mean when cyber is so unlike the other domains (for instance in being man-made)? The way to understand it is to grasp what cyberspace is, and what it is not.

Allow me to make one quick example. I recently bought an iPad. Its capability surpasses that of even NASA computers of twenty years ago. Yet the physical materials in that device are worth little in and of themselves. What makes those components valuable are the data they contain and the logical processes for making sense of those data. That value, moreover, was infused in that iPad through a series of steps that each represented a coming-together of hundreds or thousands of individual talents and contributions. Think of the highly specialized tools and materials that went into its manufacture, and then the millions of lines of computer code that comprise its operating system and programs—not to mention its applications—and you begin to grasp the complexity of our new world and the ways in which our economy and society have shifted to an information culture, where wealth is less and less rooted in the physical ability to manipulate objects than it is in the knowledge of how those objects work together.

The world is shifting its collective memory and sense-making capacity into digital forms. That wealth, moreover, exists in ways (note that I do not say places here) that are increasingly accessible by others. Time and distance are less relevant in the cyber domain than in any other. Telephones and computers and radios are essentially merging. That means our communications infrastructure is mostly computers talking to other computers. And remember that each of those computers not only moves data, it stores data—in astronomical quantities. Our radios have become our filing cabinets, and vice versa, and they have become so small that we carry them in our pockets, and there is no going back to some simpler time.

What does that mean in military terms? The cyber domain in some ways is like the air domain, in being a realm that had no relevance for military planning until all of the sudden a new technology offered access to it. A century ago the world's militaries had to learn to fight in the air, and they had to do so all at once in the midst of a world war. We realized that no one service can possess the entire air domain or claim exclusive use of it; all the services require access, all require capability, and all contribute to the joint fight. The parallels with cyberspace seem obvious: freedom of action in cyberspace, like freedom of maneuver in the air, is crucial to the efficient employment of one's forces in all domains. Likewise, the loss of such freedom could impair the capabilities we have built in all the other domains.

Cyberspace is densely populated with billions of actors. It can be difficult to sort them into friends and enemies. Indeed, everyone who logs on to the Web puts themselves into a domain that can be used not just for productive purposes, but a domain that is simultaneously a potential area for both criminal or hostile purposes. There are no sanctuaries for the innocent. When people enter cyberspace, they can be the unwitting victims of a range of malicious actors, including states' militaries. Thefts of intellectual property can take on hitherto unimaginable scale; a conqueror once had to capture a city before his army could loot it. Now that wealth is increasingly digital, economic espionage for commercial and technological advantage is an everyday event. And it is not just theft that concerns us. More and more we see states extending their use of traditional instruments of power into cyberspace. We are increasingly seeing activities in cyberspace which carry the potential to threaten national security.

In other words, competition and even conflict in cyberspace are a current reality. US Cyber Command indeed has been "in action" every day of its brief existence. The Department of Defense networks that we defend are probed roughly 250,000 times an hour. By 2006, to cite another example, the Department determined that 10-20 terabytes of data had been remotely exfiltrated from NIPRNet, our unclassified but still sensitive network that is connected to the Internet. Furthermore, while even casual users of the Web have heard of malware to monitor, exploit, and disrupt computers and networks, there are new tools appearing that can damage or destroy systems. This recent shift toward operationalizing cyber tools as weapons to damage or destroy is of great concern to us at Cyber Command.

Conflict in cyberspace, moreover, is highly asymmetric. Minor actors can afford and deploy tools to magnify their effects; witness the recent press reports about arrests in Europe of several individuals charged with creating the so-called "Mariposa botnet"—a collection of 13 million computers slaved together for criminal purposes. The tools these actors can employ are almost anonymous—a defender can sometimes learn where an attack came from, but can be time-consuming. That means "attribution" in cyberspace is costly and comparatively rare. The "price" an adversary pays for a capability—a tool or weapon—can be slight; the cost and impact borne by the victim of his attack can be very high.

Such costs can be inflicted by a nation-state's military or by one of its intelligence services, or by cyber criminals, or simply by a software glitch. Telling one actor from another and divining actors' intentions can be very difficult. Not every event that affects our networks rises to the level of a national security threat. It is important to remember that hacking, spreading malware, and other malicious activities are crimes, defined domestically as well as internationally by the Convention on Cybercrime, and accordingly have legal consequences. Even if you spot an intrusion and you know it originated from an adversary, you usually cannot tell an intelligence operation from a military one. Is a probe of your system intended by the fellow who launched it as a precursor to an effort to map your network, to steal your data, to corrupt that data, or take down the entire network? The skills to do any one of these actions are not fundamentally different from those required to do the others. The international puzzlement and concern over the seemingly innocuous Conficker worm, which has been in millions of systems since 2008, provides just a foretaste of the disruption that malicious cyber tools can cause.

Deterrence in this field is different from any other. It will not function as it did during the Cold War, as General Chilton mentioned to you last spring. Attacks by hackers and criminals can cause "nation-state sized" effects; indeed, the accidental "release" of malware might do the same, and the problem of attributing the attack to a particular actor similarly remains difficult to impossible. We have to study deterrence anew, from a variety of perspectives, and to gain clarity on our authorities. To take a thought from Sun Tzu, we must understand the cyber environment and, the capabilities of our adversaries, and our own abilities as well. This is not going to be easy, and it is not going to yield answers soon. If we know one thing from the Cold War, it is that stable deterrence can take years to achieve, and is the product of planning, analysis, and dialogue across the government, academe, and industry, and with other nations as well. Cyber deterrence will require progress in situational awareness, defense, and offensive capabilities that adversaries know we will use if we deem necessary.

US Cyber Command's Direction and Plans

US Cyber Command has three main lines of operation. We direct the operations and defense of the Global Information Grid so the Department of Defense can perform its missions, we stand ready to execute full-spectrum cyber operations on command, and we stay prepared to defend our nation's freedom of action in cyberspace.

In a strict sense, none of these jobs are new. As the Department's networks expanded and became increasingly reliant on the public Internet over a decade ago, the imperative to organize ourselves better in cyberspace became obvious. We in the United States have tried several organizational arrangements for each of those three missions, and as a result of this evolution two lessons have impressed themselves on the Department's leaders. What is new is the way in which we at Cyber Command are applying these lessons. The first is the wisdom of keeping the command and control of military networks and operations with an organization possessing a global perspective on vulnerabilities, threats, and challenges to our nation; that is why US Strategic Command, within the Department of Defense, holds authority over military operations in cyberspace and delegates it to US Cyber Command. The second lesson we have learned has been the need for a tight synchronization between the people who monitor and operate the Department's 15,000 networks and their colleagues who watch and respond to adversarial activities. In short, several previously parallel streams of expertise have to blend together continuously or leadership will not have crucial situational awareness and a full range of options.

The price we might pay for not having such synchronization can be high. An incident in late 2008 underscored this point for Departmental leadership, and also helped us to fashion a template for "operationalizing" our management of the Department's sectors of cyberspace. Operation Buckshot Yankee was our response to a very serious infection of a classified network serving US Central Command. What happened was that contaminated thumb drives were used by US military personnel in the Middle East who had no idea they were implanting malware created by one of the more than one hundred foreign intelligence services seeking to break into our systems. The resulting infection amounted to what Deputy Secretary Lynn called a "digital beachhead" on our networks that could have been dangerously exploited by an adversary if it had not been detected, analyzed, and neutralized by a combination of intelligence and military efforts. The malware involved demonstrated the skill and determination of our adversaries, and hence the urgency for increasing our preparedness for the next attempt to penetrate our sensitive systems. At the same time, our response in Operation Buckshot Yankee convinced leaders in the Department of Defense of the potential for synergy that results from combining network operations with dynamic defenses and the ability to play offense as well.

Operation Buckshot Yankee should have vanquished any notion that Department of Defense networks are not at risk. The Deputy Secretary has enumerated five principles for the Department's strategy in cyberspace, and these guide our efforts as we build US Cyber Command and launch its operations. Cyber Command is not the sole participant in any of these fields of effort, but it is a leader in collaboration with its mission partners in all of them:

- *First, remember that cyberspace is a defensible domain*. We should study cyberspace in the same way we study the other domains, to understand how the principles of the military art apply there. We must learn its topography, so to speak, along with its environmental challenges and culture, just as we would seek to learn about any other "place" where we might have to defend our nation and its interests. Let me offer an example of the work that remains to be done. The Department has learned through experience to organize its operating forces in the field not by Service but by mission, with each geographic combatant commander controlling components and task forces that operate in one or more of the domains within his region. US Strategic Command stretches this mold slightly, in controlling forces possessing global reach (and the use of which always implicates national interests). This exception, however, proves the rule in being a supplement to the work and the capabilities of the geographic commands—available to meet their needs for longer-ranged and more-powerful support. Command and control in cyberspace is still more complicated. Computer network operations can be regional and global at the same time, and can have effects approaching those of weapons of mass destruction. The devices that give us access to cyberspace exist in the physical world, and in conventional military terms we can say that they are always within the area of responsibility of some geographic combatant command—but they can create effects that take place far away in the area of responsibility of a second command, and they might be enabled to do so by unsuspecting users and their devices located in still a third command's region. Which commander is the mission lead in such a case and is military action appropriate? Which command is supported, and which is supporting? In cyberspace, questions like this must be answered at Internet speed and must take into account our responsibilities and obligations under international law and norms. For example, the U.S. has affirmed that the international Law of Armed Conflict, which we apply to the prosecution of kinetic warfare, will also apply to actions in cyberspace. Of course, the details of this remain to be developed in light of the unique attributes of Internet technology. Indeed, in cyberspace a command can be supported and supporting at the same time, with the roles switching back and forth. The trick is to engineer a structure for operations in cyberspace that combines the necessary processes, immediate feedback, and effective controls with sufficient elasticity to respond when the first warning might be fragmentary but the risk of waiting even a few minutes for better information can be grave.

- *Make our defenses active* – In cyberspace the only "perfect" defense is the static one: to disconnect and thereby forfeit the cyber realm and its economic and social benefits to one's adversaries. That is not possible for the United States or the Department of Defense. Indeed, there is no "unplug" option for American society; our homes, businesses, schools, hospitals, government offices, and indeed our very way of life now depend on access to networks. Even if you do not own a computer, you rely on neighbors, colleagues, and institutions that do. Our cyber engagement is thereby a matter of prudent vulnerability management and risk recognition. Since security in a networked world is a system for managing that risk, we in US Cyber Command have a structured system of security measures for Departmental networks: monitoring of the Grid for situational awareness, advisories and patches and updates, anti-virus programs, firewalls, objective security assessments, automatic intrusion detection and blocking measure, active searches for malware, and forensic response teams. We manage all this with what we call Dynamic Network Defense Operations, and it is a cornerstone of our work.

- *Extend protection to our critical infrastructure* – About a generation ago the infrastructure that undergirds our society and economy passed a tipping point when computers ceased to be optional features and became essential for basic functioning. President Obama has made guarding that infrastructure a national security priority. Today our energy sources, utilities, public transportation, banking, public records, and much more are all on "the Net." Our military, furthermore, depends on unclassified networks for much of its communications and logistical functions. While automation and networking make the command and control of such systems more convenient, it adds a dimension of complexity and concomitant vulnerability that the creators of these systems never anticipated. Because of that, the legacy systems that run much of our critical infrastructure are inherently more difficult to protect and defend than modern systems being created today. No one has seriously attacked these yet—at least not in the United States—but we have seen the probing of those systems by our adversaries. We have seen enough evidence of their vulnerability due to natural disasters and accidental malfunctions—like the software glitch that contributed to the power outage across the

Northeast in August 2003—to be concerned about the potential effects of an actual attack on any piece of the networked infrastructure. The Department of Homeland Security has the daunting task to work collaboratively with public, private and international entities to secure cyberspace, and America's cyber assets, systems, and our colleagues there are moving out toward that end. But the need is great and there is no time to lose, as attacks and their potential effects would not discriminate between military and civilian users, and could come from a nation-state adversary, a terrorist group, or even a rogue individual. The Department of Homeland Security may require expert advice and consultation from both NSA and Cyber Command; both organizations stand ready to assist. Further, in the event of an attack we need to practice coordinated response efforts across government.

- *Foster collective defenses* – I like to call cyber a team sport; successful defense in any one part depends on the shared efforts of agencies, industry, allies, and mission partners who watch their own networks for problems that could affect them all. Each of us, and our colleagues, co-workers, friends, and families, are all participants—and potential targets. To avoid becoming victims, we must take positive and frequent steps to prevent that outcome. We are all part of a combined solution to a common problem. We can all do our part to understand the complexity of our new world and reduce our shared vulnerability. Many of the problems that keep us at work nights and weekends would be substantially diminished if users at their homes and offices would download and install manufacturers' recommended patches and updates. That is nothing new—many others have made the point before me. But the fact that it has to be repeated suggests something else that is different about cyberspace—it's tough to "see" security in the way we can see locks and bars and guards. Security is always inconvenient, and even more so in cyberspace because it costs time to get right and keep up-to-date—which is much of the battle right there. The cost of successful attack, however, is much higher than the expense of connecting and deploying the hardware and software to stay connected. Making security work requires common standards and terminology and the sharing of great quantities of timely information. We at Cyber Command have strong and tested military and intelligence partnerships with our allies that help us all in forming a common operating picture, and we are seeking to expand that ring of partnerships. None of us have all the authorities, capabilities, or resources to go it alone. We must work together.

- *Leverage US technological advantages* – The United States did much of the pioneering work that built the first computer data sharing networks, and many innovations in the hardware and software sectors still arise in this country. Our lead, however, has never been purely technological. I am convinced that the solutions to our vulnerabilities in cyberspace will prove to be primarily cultural and procedural. We do not necessarily need "better" technology than the proverbial other guy, in terms like bandwidth, storage, software versions, operating speeds, memory size, and so on. In any case, purely technological advantages are likely to be fewer and less lasting in our networked world. Our advantage has to lie in how we put these tools together in systems, especially systems of people, protocols, and machines that can operate reliably together at high speeds to identify vulnerabilities, share information, assess risks, devise countermeasures, and apply new solutions. Although US Cyber Command will not have acquisition authorities, we will support US Strategic Command in defining requirements. We in

Cyber Command are also participating in the Enduring Security Framework, a group of officials representing the Secretaries of Defense and Homeland Security and the Director of National Intelligence, who meet regularly with leaders from the private sector and experts in the cyber field. We envision this partnership as essential to helping the public sector address the cyber security threat. In addition, we are working with the Defense Advanced Research Projects Agency and supporting a "National Cyber Range" environment to build our capabilities in this field. Finally, another imperative is to build the capability of our "cyber workforce" in the Service cyber elements. They are essential to the accomplishment of our mission of supporting the combatant commands and national requirements. I cannot overemphasize the need for this workforce, and this capacity, to be built as soon as possible.

Conclusion

I thank you again for calling me before you today and giving me this opportunity to submit the first posture statement for US Cyber Command. I am convinced we have taken an important step for our nation in creating this Command, and that we have done so not a moment too soon. I have described our philosophy of actively managing the Global Information Grid—not just to defend it, but to use it as a tool to assist our warfighters, planners, and commanders by keeping their freedom of action as broad as possible—and of being as ready as we can, and when called upon, to use our own capabilities to disrupt any adversarial use of cyberspace against the United States, its interests and critical infrastructures, or other governments. I pledge that we will pull this new Command together in compliance with all of the laws governing privacy and civil liberties of U.S citizens, in accord with the directives of the national command authority, and, in conjunction with our mission partners in the Departments of State, Defense, and Homeland Security, law enforcement, the Intelligence Community, and industry and academe. We have to get this right, as I believe the security of our nation depends on it. We are working to meet this challenge so as to be worthy of your trust. With your help and counsel I have no doubt that we can succeed. I look forward to your questions.