

UNCLASSIFIED

Statement for the Record

Lieutenant General Keith Alexander

Commander

Joint Functional Component Command for Network Warfare

Before the

House Armed Services Committee

Terrorism, Unconventional Threats, and Capabilities

Subcommittee

5 May 2009

UNCLASSIFIED

(U) Introduction

(U) Chairman Smith, distinguished members of the committee, thank you for the opportunity to discuss the military's cyberspace mission and some of the challenges we face executing the responsibilities assigned to us by United States Strategic Command (USSTRATCOM).

(U) Background

(U) As you are all well aware, our economy, the nation's critical infrastructure, and many of our military operations depend on unfettered access to cyberspace. Cyberspace has clearly changed the way we interact as a global community. More than that, it has influenced business processes, the management of critical infrastructure, and human interaction in ways that were not foreseeable just 15 years ago. However, this advancement in technology comes with vulnerabilities for our nation that have not been adequately addressed.

(U) The vast array of electronic devices populating the global information infrastructure today remain the functional tools of cyberspace, and any of these devices, or the underlying software, can be used for both beneficial or malicious purposes. As cyberspace continues to evolve and grow in complexity and importance, our nation must vigilantly maintain technological dominance and freedom to maneuver within this global domain. This statement will focus on the latter in an attempt to provide this Committee insight into how the DoD is organizing to operate in the cyber domain, how we operate in the environment and some initial thoughts regarding deterrence.

(U) JFCC-NW Organization Overview

(U) As the Commander, Joint Functional Component Command for Network Warfare (JFCC NW), it is my responsibility to support USSTRATCOM's mission to plan, coordinate, and conduct offensive and defensive cyberspace operations. Executing this mission requires assembling and maintaining a force capable of adapting to, and operating in, a complex and continually evolving and expanding environment. Unlike the land, sea, air and space where the laws of physics do not change, cyberspace is a man-made creation that continually changes and evolves – operating effectively in this kind of environment requires that we leverage the expertise from a wide variety of disciplines. Moreover, we must close the seams between information assurance, network operation and defense, intelligence collection and offensive operations. Recently the Commander, USSTRATCOM, placed the Joint Task Force – Global Network Operations (JTF-GNO), which directs the operation and defense of DoD's networks under my operational control in order to better integrate and synchronize defensive cyber operations. This necessary initial realignment is a significant step towards the establishment of a command that is organized to operate and defend vital networks and project power in cyberspace.

(U) The next steps in this transformation will require a more substantial reorganization, which is one reason why the DoD is considering the establishment of a new sub-unified command for Cyber, under USSTRATCOM, that would be headquartered at Fort Meade. The creation of a single, sub-unified cyber command would provide the DoD with a command comprised of forces and capabilities better aligned to conduct cyber operations and capable of evolving to meet and overcome challenges presented by operating in cyberspace at the speed of cyber.

(U) Operating in Cyberspace

(U) Maintaining freedom of action in cyberspace in the 21st Century is as inherent to U.S. interests as freedom of the seas was in the 19th Century, and access to air and space in the 20th Century. This is especially true since the United States is committed to leading international and domestic efforts to ensure the security of global information infrastructures upon which cyberspace depends; maintaining the capabilities to use cyberspace as a medium to deter, deny, or defeat any adversary seeking to harm U.S. national and economic security; while ensuring actions are undertaken in a manner that protects our Constitutional liberties. The ability to operate freely within cyberspace poses a number of unique challenges.

(U) The rapid expansion and global dependence upon cyberspace required the Defense Department to evolve its warfighting doctrine to include cyberspace as a viable domain on par with the domains of the land, sea, air and space. As I have mentioned, cyberspace is unlike the other warfighting domains, it is a man-made technological phenomenon solely reliant upon human activity. The Department of Defense defines cyberspace as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processes and controllers.”¹

(U) The uniqueness of cyberspace can best be described by three attributes: volume, speed, and convergence.

(U) Perhaps the characteristics of volume and speed are best known, as the truly unprecedented volumes of data and speed at which communications occur in cyberspace are demonstrated daily. More than the speed of the communications, the rate of change of cyberspace, and the applications that use it, is continuous, making this domain ever evolving. However, the convergence of communications devices being driven by cyberspace is fueling an integration that has far reaching consequences, both positive and negative, that must be appreciated if one is to understand this domain.

¹ See Deputy Secretary of Defense Memorandum, Subject: *The Definition of Cyberspace*, May 12, 2008 (The Department of Defense holds this definition is consistent with the definition of cyberspace provided in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23), which states that cyberspace is “the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.”)

(U) The integration taking place in communication devices is easy to see in our daily lives. What were once separate communications means such as telephones, cell phones, television, radio and computers are increasingly being combined into single devices, allowing us to watch video or send email on our cell phone or use the telephone over the Internet. Fundamentally, this is only possible because of a much greater integration occurring behind the scenes, the increasing merger of what were once separate communication networks into one network-of-networks. Accordingly, what were once distinct networks carrying the communications of our adversaries, allies and ourselves have also merged into one network-of-networks – “cyberspace”.

(U) And while it may be hard to believe for something that has become so important and so much a part of the fabric of our lives, cyberspace largely “happened.” It was not planned or designed to serve the purposes for which it is being used today. And while the concept to make it easier for people to communicate by connecting networks was conceived and given life in the United States, it resulted in a global domain that knows no geographical boundaries, is largely unregulated and impossible to fully secure. There is no one entity, be it from the private sector or from the community of nations, “in charge” of cyberspace, which means that there is no one entity that can change cyberspace to eliminate the negatives while keeping the benefits. Thus, cyberspace is a perfect environment for United States adversaries to thrive and a domain that the United States must vigilantly protect.

(U) Deterrence Strategies

(U) Robust information assurance and securing vital networks must be our first priority. Our people play an important role in preventing unauthorized access to the critical systems in cyberspace. The cyber security training provided to our service men and women, and the civilian and contractor workforce is inadequate and must be improved.

(U) Secondly, the defense of our networks must be accountable to the highest levels, and managed as such. It is imperative that all commanders enforce measures to ensure the readiness of networks managed by personnel under their purview. Our adversaries are taking advantage of this lack of assiduousness and discipline that ultimately costs hundreds of millions of dollars in lost information and work hours.

(U) Finally, we must leverage the power of automated security protocols to effectively manage these threats we face every day. For example, deploying a host based security system will provide a level of security that potentially will operate at the speed of the network, and centrally update systems to a trusted baseline.

(U) Conclusion

Cyberspace is a uniquely complex domain absolutely vital to the nation. For the Department of Defense to operate freely within the cyber domain it must devote sufficient

UNCLASSIFIED

resources and personnel to ensure mission success. This includes creating an organizational construct that aligns and synchronizes forces so that they are able to operate and defend the military's network and project power at "network speed".

Traditionally, military action is an option of last resort that should complement deterrence strategies. Within the DoD, deterrence can be partially achieved through the creation and maintenance of a cyber force capable of freely operating within cyberspace.

Thank you for providing me with this opportunity and I will try to answer any questions that you may have.