RECORD VERSION

STATEMENT OF

MAJOR GENERAL RHETT HERNANDEZ, USA

INCOMING COMMANDING GENERAL,

U.S. ARMY FORCES CYBER COMMAND

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES

2ND SESSION, 111TH CONGRESS

SEPTEMBER 23, 2010

NOT FOR PUBLICATION
UNTIL RELEASED BY THE
HOUSE ARMED SERVICE COMMITTEE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND
CAPABILITIES

Major General Rhett Hernandez, USA
Incoming Commanding General
U.S. Army Forces Cyber Command

Introduction

Chairwoman Sanchez, Ranking Member Miller, and Members of the Subcommittee, thank you for your ongoing support of our military and for the opportunity to appear before this panel with my counterparts from the other Military Services. Your support is important as we strive to mature and enhance our cyber capabilities. As the former Director of National Intelligence stated in his February 2010 annual threat assessment before the Senate Select Committee on Intelligence, “our economic prosperity and the daily functioning of our government are dependent on a dynamic public and private information infrastructure, which includes telecommunications, computer networks and systems, and the information residing within.” Freedom of movement in cyberspace is a national security imperative for our Nation and our allies. Information technology, as Deputy Secretary of Defense Lynn stated so succinctly, “enables almost everything the U.S. Military does.”

Army Forces Cyber Command (ARFORCYBER) is the Army’s service component in support of U.S. Cyber Command (USCYBERCOM), a sub-unified command under U.S. Strategic Command (USSTRATCOM). Our mission is to plan, coordinate, integrate, synchronize, direct, and conduct network operations in defense of all Army networks and mission objectives. We stand ready, when directed, to conduct those cyberspace operations necessary to ensure U.S. and allied freedom of action in cyberspace.

As the Army’s service component, my headquarters will coordinate with USCYBERCOM to organize, train, and equip effective cyberspace forces to support all USCYBERCOM Lines of Operation. We will also support USCYBERCOM with prioritization, coordination, and validation of Army mission requirements and force capabilities. This synchronized relationship will enhance situational awareness and achieve more effective coordination across the spectrum of cyberspace operations. Further, when USCYBERCOM directs, we will support establishment of Joint Task

Forces. Finally, ARFORCYBER will provide shared situational awareness of the Army's portion of Department of Defense (DoD) information networks to support cyberspace operations so the Commander, USCYBERCOM, can effectively command and control operations using a common Joint operational cyber picture.

As the incoming commander of ARFORCYBER, I will also work to ensure the Army closely coordinates with the other Services and the Combatant Commanders to ensure the Combatant Commanders receive the cyber operations support they require to accomplish their Joint missions.

Background

Before I discuss the details of where we are and where we are going in the cyberspace mission, I would like to share with you some of the decisions previously made by Army leadership that have positioned us to move forward quickly as we stand up ARFORCYBER. In 2004, recognizing the critical collaboration required between network defenders and providers to secure Army networks, the Army combined the Army Computer Emergency Response Team (ACERT) and the Army Global Network Operations and Security Center (AGNOSC) into a single Threat Operations Center at Fort Belvoir, Virginia. This new and collaborative organization ensured not only a robust defense of the network, but also the ability to protect the integrity and validity of both the networks and the content stored on them.

By September 2006, the Army recognized that computer network operations were evolving into the larger mission set of cyberspace operations. It therefore directed 1st Information Operations Command to integrate, coordinate, and synchronize Army computer operations. There remained, however, a requirement for senior operational leadership to oversee this mission.

To address this requirement, the Army, in January 2008, designated the Commanding Generals for Network Enterprise Technology Command (NETCOM)/9th Signal Command (Army) and U.S. Army Intelligence and Security Command (INSCOM) as Deputies for Network Operations and Network Warfare respectively under the Commanding General, U.S. Army Space and Missile Defense Command/Army Forces

Strategic Command (USASMDC/ARSTRAT). This new structure put an operational three star general in charge of Army computer network operations and provided the capabilities required across the spectrum of computer network operations.

On June 23, 2009, the Secretary of Defense issued a memorandum directing each of the Services to identify before the targeted fully operational capacity date of October 2010 an appropriate component to support USCYBERCOM. In response to that memorandum, this past year the Army named USASMDC/ARSTRAT as its Service Component in support of USCYBERCOM.

Foreseeing, however, the increasing global scope of the cyberspace mission, the Army determined it needed an organization focused solely on cyberspace operations. In February 2010, the Army approved the recommendation to stand up a separate command focused on the cyber mission. On October 1, 2010, ARFORCYBER assumes the cyber mission and brings unprecedented unity of effort and synchronization of all Army forces operating within the cyber domain.

In summary, over the past decade various elements within the Army have undertaken significant initiatives for network, information, and computer network operations. These initiatives, however, lacked the unity of command and control necessary to fully integrate them in support of DoD and National cyberspace operations. ARFORCYBER is organized to link Army networks worldwide, to fully integrate Army Computer Emergency Response Teams, and to draw upon INSCOM's cyberspace forces and capabilities. Reorganizing the Army's existing resources for cyber operations under a single command provides us the ability to serve as an operational arm to USCYBERCOM in support of its mission.

Cyber Operations

Our primary mission is to support USCYBERCOM in its defense of DoD networks and our Nation. To succeed in this endeavor, we must be able to operate in a joint environment that includes not just USCYBERCOM, the Component Commands, and our sister Service Components, but also other departments, agencies, and private entities. Therefore, as USCYBERCOM establishes its operating procedures, ARFORCYBER must concurrently establish and grow effective linkages with our sister Services. I expect to achieve a balance between centralized coordination and planning at USCYBERCOM and the routine exchange of operational data, planning, and resources with our sister Service elements. Internally, the Army must balance the centralized command and control exercised by ARFORCYBER against theater missions, responsibilities and priorities. As an operational force, the Army has strong competencies in the cyber arena: global presence, expeditionary experience and full-spectrum capabilities. We will effectively integrate our capabilities into USCYBERCOM's joint operational and planning efforts so we can fully support USCYBERCOM's joint missions.

The Army excels at achieving traditional military effects to support commanders' objectives. In the global cyber domain, however, with operations occurring at net speed across national boundaries and often involving multiple state and non-state actors, tactical actions can result in unforeseen and grave strategic consequences. Attributing adversary activity creates challenges, and collateral effects are often equally difficult to predict and fully understand. Our adversaries benefit from operating in a relatively unrestrained environment.

These cyberspace concerns and constraints require us to undertake more robust measures to defend our networks and National cyber interests. To effectively defend our networks and deter and oppose our adversaries, we must continue to grow our intelligence and cyber operations capabilities. This will require continued commitment on a national strategic scale. We must also establish internal processes and procedures within and between the Department's cyber organizations to enable cyberspace activities under various authorities to work in concert with each other to more effectively support cyber operations.

Fundamental first steps in achieving these goals include improving our ability to see and understand our networks better. We will do this by collapsing our networks from a disparate, loose federation into one Army enterprise network. This will enable us to establish centralized control of our networks and give us more complete, integrated visibility into them. Having accomplished this, we can then establish an active defense in depth across the network.

People, however, are the centerpiece for all efforts to improve our ability to operate effectively in cyberspace. The first line of defense in cyberspace is the user. To operate effectively, we must change our culture. Every individual must understand cyberspace is a contested environment that must be protected. The second line of defense is our corps of cyber professionals who defend our networks and ensure operations. We will win the contest in cyberspace as we win on traditional kinetic battlefields, with the best trained and most professional personnel. To that end we must increase our capacity to grow cyber professionals and to retain them. Many resources, including time and money, are necessary to train the cyber workforce required for today's environment. Once trained, our challenge is to retain them. Their skills are highly marketable throughout the public and private sectors. The importance of retaining our highly trained cyber professionals cannot be understated – doing so is essential to maintaining our ability to effectively conduct cyber operations.

Organization for Cyber Operations

To efficiently and effectively accomplish its cyberspace missions, ARFORCYBER is organizing as indicated on the attached organizational chart. It will include NETCOM/9th Signal Command (Army), and operational control of cyber forces assigned to INSCOM. The newly formed Army Cyber Operations and Integration Center (ACOIC) will be the focal point of our command and control and synchronization.

The Commanding General, NETCOM/9th Signal Command (Army), will serve as the ARFORCYBER Deputy Commanding General for Network Operations and Defense. In this capacity, she controls four Theater Signal Commands which support respectively, the U.S. Northern and Southern Commands, U.S. Pacific Command, U.S. Central Command, and the U.S. European and Africa Commands, as well as a Signal Brigade in support of U.S. Forces Korea. These forward deployed Signal Commands and the Signal Brigade are unique to the Army and give ARFORCYBER a forward network operations command and control presence in these theaters.

The Commanding General, INSCOM, will serve as the ARFORCYBER Deputy Commanding General for Network Warfare. She will control forces, to include a Cyber Brigade being established to provide dedicated support to ARFORCYBER, which support cyber operations and intelligence requirements.

Army Cyber Operations and Integration Center **(ACOIC)**

The ACOIC is the command and control center for all Army service-related cyberspace activities. Using current and evolving doctrine and lessons learned from enduring and future operations, the ACOIC will ensure Army personnel at all levels receive clear, concise, and timely direction to execute full spectrum operations in cyberspace. The ACOIC also integrates the process for Army personnel and organizations to report anomalies in the cyberspace domain. The ACOIC is postured to maintain close watch on all Army cyberspace operations that may impact our national security and to share that information with other Army commands, our counterparts in the other Services, and the U.S. Cyberspace Joint Operations Center.

To ensure the ACOIC is fully nested with and able to seamlessly support USCYBERCOM, the ACOIC is physically locating and embedding approximately 25 personnel in the USCYBERCOM joint staff. These embedded personnel will ensure close collaboration with USCYBERCOM and enable the ACOIC to leverage USCYBERCOM's unique resources and capabilities. As the Army continues to seek advancements in cyberspace operating capabilities, the ACOIC will serve as the hub for advancements to materialize. It will include trained personnel dedicated to future planning, capabilities assessment, and exercises and training. This organizational structure will ensure the Army remains prepared with properly trained and equipped personnel to effectively respond to current and future challenges awaiting in cyberspace.

Future challenges will include the speed and consequential global impact of events in cyberspace. The boundaries of cyberspace are, of course, often unclear. Several factors (e.g. ownership of equipment, users of equipment, and location of equipment) influence the interpretation of where cyberspace boundaries lie. To further complicate such determinations, a cyberspace event may simultaneously occur in multiple geographic locations. The ACOIC will assist the USCYBERCOM Joint Operations Center to maximize global availability of cyberspace for the DoD and its coalition partners and allies.

Training

Our national and military dependence on the cyber domain and information technology demands that we invest in cyber capabilities to grow the skills necessary to maintain our ability to operate freely in cyberspace. A significant number of our command and control and logistics systems depend on cyber technologies. We must therefore make significant investments in education, training, and experience to understand emerging trends, develop and deploy new capabilities, and effectively defend against new cyberspace threats.

In addition to training sponsored by Army organizations, such as the Basic Computer Network Operations Planners Course, the Army leverages Joint cyberspace training courses such as the National Security Agency's System and Network Interdisciplinary Program.

Recognizing the Army's unique cyberspace training requirements, the U.S. Army Training and Doctrine Command initiated a formal "Cyberspace/ Electromagnetic Contest" Capabilities Based Assessment in February 2010. This assessment, which is being led by the U.S. Army Combined Arms Center at Fort Leavenworth, Kansas, will provide additional analytic insights for evaluating Doctrine, Organization, Training, Material, Leadership, Personnel, and Facility (DOTMLPF) gaps and solutions across all echelons of the Army. This effort will result in a comprehensive assessment of the training and personnel requirements necessary to conduct effective cyberspace and electromagnetic spectrum operations. We expect to receive the results of the Capabilities Based Assessment over the next year.

Personnel

To fully establish ARFORCYBER's headquarters, the Army will locate the headquarters in the National Capital Region and will realign Soldiers and civilians into essential ARFORCYBER headquarters positions. The total command strength of 21,000 Soldiers and civilians will be located around the globe. ARFORCYBER will include personnel currently assigned to the NETCOM/9th Signal Command (Army), portions of the 1st IO Command (Land), as well as with resources from USASMDC/ARSTRAT. Additionally, cyber operations personnel from INSCOM will support ARFORCYBER for cyber-related actions.

Manning levels for the Headquarters and the ACOIC were determined through an extensive analysis of existing and new mission sets, comparative analysis with other Services' cyber organizations and manpower studies. As the organization matures, manning levels will be evaluated against the "Cyber/ Electromagnetic Contest" Capabilities Based Assessment, as well as a follow-on manpower study that will be conducted within the next 18 months.

Technology

The current Army network is a loose federation of regional and command-centric enterprises with disparate levels of security, network visibility, and control. The first step on our cyber technology roadmap is to have the capability to "see" the network. The Army is achieving this by moving our networks to centralized control, and then instrumenting the network with a common tool set that can produce a predictable and repeatable picture of what is happening. This will transform the Army managed LandWarNet into a single Army Enterprise Network that standardizes security posture, establishes visibility, and allows for seamless transition of forces between the generating force and combat deployments. While these tools are designed to present a picture of the network's health and welfare, they do not completely inform commanders about what is happening in the network.

The next step is to "understand" what is happening on our network through real time situational awareness, single reporting, shared visibility, and a proactive defense.

This will allow operational commanders to make risk-based decisions in the context of complex multi-domain operations. This extended reporting and awareness will, in turn, enable higher level commanders to better assess risk in the context of theater or global implications and then take the appropriate action at the proper level to enable mission assurance within cyberspace.

The final step is to have the capability to "understand" what we "see" and "do" something about it before the threat can gain an advantage in the cyberspace domain. We can achieve this through the integration of full spectrum cyber operations. Once we can see and understand our network environment well enough to proactively operate and defend against threats at "net speed," we can start leveraging cyberspace as a domain in which the joint force commander can maneuver.

To fully leverage cyberspace as a domain, we must constantly strive to harness new technologies. To do this, ARFORCYBER will pursue innovative Army acquisition processes that allow us to keep pace with rapidly changing technologies without risking the fiscal integrity of the acquisition system. Several Congressional, DoD, Combatant Command, and Service studies have shown that developing and refining cyberspace related Rapid Acquisition Processes is critical to achieving and maintaining superiority in cyberspace. For example, acquisition cycles that normally take two or more years will not satisfy critical mission requirements.

The Army must focus on three areas. First, we must establish a cyberspace science and technology program that leverages emerging capabilities from both the private sector and academia. Second, the Army must pursue and implement cyberspace-specific acquisition and procurement policies that allow the warfighter to conduct research, development, testing, and evaluation of promising cyber technologies in an extremely efficient time line. Finally, the Army needs a rapid development and fielding process nested within the Army’s Combat Development for Rapid Equipping processes that have been so successful in equipping the force in Afghanistan and Iraq. Without the ability to leverage cyberspace science and technology advancements, the authority to promptly conduct research, development, testing, and evaluation, and the means to rapidly transition successful technologies, the Army and the joint warfighter will struggle with the need to quickly acquire technology and infrastructure necessary for responding to gaps and threats from our adversaries.

Doctrine

As the Army integrates cyberspace into current and future force structure and operational concepts, we must meet the challenge of how to integrate our efforts into full spectrum operations and address both the generating force and the operating force. U.S. Army Training and Doctrine Command has coordinated concept development for cyber with stakeholders across the Army, and in January of this year published a Cyberspace Operations Concept Capabilities Plan (CCP) which outlines the framework under which the Army expects to conduct cyber operations in the timeframe 2016-2028. The CCP was the first step in the ongoing Capabilities Based Assessment for cyber and is nested closely with updates to Army doctrine for command and control and synchronized with the revision of Field Manual 3-0, Operations, the Army's Capstone doctrine for operations.

As we gain experience in cyberspace operations and improve our capabilities, Army cyber doctrine development must remain closely nested in broader Joint doctrine. The Army, along with the other Services, has participated in USSTRATCOM's development of a draft Joint Test Publication for Cyberspace Operations. Additionally, the Army has been working very closely with the sister Services and the Joint Staff in support of USSTRATCOM's Cyberspace Joint Operating Concept initiative.

We are at the beginning phase of the process to develop and document operational concepts and a robust doctrinal framework for cyber. Our Nation, the DoD, and the Joint Warfighters will require new and updated policy, concepts, and doctrine to effectively combat intelligent, evolving adversaries who are leveraging cyberspace to enhance their capabilities. To fight and win future battles, we must not only out-maneuver our potential adversaries, we must out-think them strategically, operationally, and tactically.

Conclusion

Ms. Chairwoman and other members of the subcommittee, I want to end by thanking you for your continued support to the Army and our Nation. As I assume command, I pledge my support to you and our Nation. Please rest assured that the Army, in conjunction with the Department and the other Services, stands ready to defend and protect our Nation’s digital infrastructure. I appreciate having the opportunity to speak on these important matters and look forward to addressing any questions you or other subcommittee members may have.