

STATEMENT BY

LIEUTENANT GENERAL RHETT HERNANDEZ
COMMANDING GENERAL
U.S. ARMY CYBER COMMAND/2ND ARMY

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

CONCERNING DIGITAL WARRIOR: IMPROVING
MILITARY CAPABILITIES IN THE CYBER DOMAIN

SECOND SESSION, 112TH CONGRESS

July 25, 2012

NOT FOR PUBLICATION
UNTIL RELEASED BY
THE HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Chairman Thornberry, Ranking Member Langevin, and members of the Subcommittee, thank you for your ongoing support of our military and for the opportunity to tell you about Army Cyber Command. I am honored to represent the required staff of 561 Soldiers and civilians, whose great work enables our Army's ability to operate everyday and adds to our Nation's security. I am humbled and proud to serve with them, and amazed at what they have accomplished and continue to do daily to address cyberspace challenges and opportunities.

Much has happened since I last spoke to this Congress in September of 2010, before activating the command. The men and women of Army Cyber Command have been hard at work increasing the command's capacity and capability, securing and defending all Army networks, conducting cyberspace operations in support of USCYBERCOMMAND (USCC), and preparing the Army to prevent, shape, and win in and through cyberspace.

The Secretary of the Army created the United States Army Cyber Command/2nd U.S. Army pursuant to General Order 2010-26, establishing it as an operational-level Army force reporting directly to Headquarters, Department of the Army. The Command attained full operational capability on October 1, 2010. Army Cyber Command is the lead for Army missions, actions and functions related to cyberspace, and responsible for planning, coordinating, integrating, synchronizing, directing and conducting Army network operations and the defense of all Army networks. When directed, Army Cyber Command conducts a full range of cyberspace operations to ensure freedom of action in cyberspace, and to deny the same to our adversaries. Army Cyber Command serves as the single Army point of contact for reporting and assessing Army cyberspace incidents, events, and operations and for synchronizing and integrating responses thereto.

The Secretary of the Army has also assigned responsibility for conducting the Army Information Operations (IO) mission to Army Cyber Command. As cyberspace is a global domain within the information environment, having a single three-star Command responsible for both cyberspace and information operations allows for the necessary integration in support of these two mission areas.

Army Cyber Command also serves as the Army's force modernization proponent for cyberspace operations and is responsible for the development of required Doctrine, Training, Leader Development, Organization, Materiel, Personnel, and Facilities.

The Command is a split-based command, with the Headquarters at Fort Belvoir, Virginia, with select staff elements at Fort Meade, Maryland. The Headquarters is has a required strength of 561 personnel and a current strength of 509 personnel. Other Army Commands supporting our efforts include the U.S. Army Intelligence and Security Command (INSCOM), Fort Belvoir, Virginia; the 1st Information Operations Command (Land) (1st IO), Fort Belvoir, Virginia; and,

the U.S. Army Network Enterprise Technology Command/9th Signal Command (Army) (NETCOM), headquartered at Fort Huachuca, Arizona. Together these units provide more than 21,000 Army Soldiers, civilians, and contractors in support of cyberspace and information operations worldwide.

Army Cyber Command and its supporting units are in action every day securing and defending Army networks and conducting cyberspace operations critical to DOD and Army missions. To defend and advance our national interests, Army Cyber Command must, like the entire Army, balance resources and risk to perform the Army's three roles: prevent conflict by maintaining credibility based on capacity, readiness, and modernization; shape the environment by sustaining strong relationships with our military allies in other nations, building their capacity and facilitating U.S. strategic access; and, win decisively by applying combined arms capabilities to dominate the operational environment.

As the Army looks toward its future, we must continue our fundamental transformation to meet the challenges of the 2020 strategic environment. This transformation must include the development of Cyberspace Warriors and organizations able to use cyberspace to gain advantage over threats to seize, retain, and exploit the initiative. Cyber Warriors and formations will help joint force commanders prevent or deter conflict, prevail in war, and create the conditions for favorable conflict resolution by being trained, organized, and equipped to conduct, as directed, the full range of cyberspace operations.

Cyber Threat

We all recognize that cyber threats are becoming more dangerous and are on the Intelligence Community's list of biggest challenges to our Nation. These threats are real, growing, sophisticated, and evolving. There is a wide range of actors ranging from lone individuals to organized hacker groups, criminal syndicates, violent extremist organizations, and sophisticated nation-states. All pose a danger of increasing their ability to disrupt the networks or critical infrastructure we count on to operate and conduct missions, and advancing their techniques to exploit our people and information. Others are seeking more disruptive or potentially destructive capabilities to impact our freedom to operate and our national security. Collectively, these threats create a dynamic and dangerous cyberspace environment.

Daily there are thousands of attempts to penetrate Army networks. Each Army computer faces multiple unauthorized attempts a day to penetrate Army networks. End users remain our most vulnerable link. Every time Army Soldiers and Civilians enter the network, regardless of where they are, they must recognize they're in a contested environment. Everyone must be aware of the cyberspace threats and remain vigilant against them.

Defense of All Army Networks

Army Cyber Command's primary focus is to secure and defend all Army networks. Serving as the Army's service component to USCC has provided unprecedented unity of effort in defending DOD and Army networks. Their ability to stop threats before entering our networks has added to an integrated, defense in depth.

Over the past 22 months, Army Cyber Command has blocked more than 400,000 attempts by individual internet protocol addresses to gain unauthorized access to Army networks; 4,000 known bad/malicious websites; 400 email phishing campaigns from accessing Army computers. On average, we block 64 million internet protocol addresses and 4,500 web sites daily and add more to the list weekly.

Enterprise Email transition continues, with more than 330,000 Army e-mail accounts completed. Common Access Card users will authenticate and access email services from centralized DOD data centers, and connect from anywhere in the world. This service provides a single identity, with a single internet protocol address, increasing effectiveness and strengthening the security of our networks.

Our work on compliance has improved Information Assurance, reduced vulnerabilities, and mitigated risk to operations. Our Web Risk Assessment Team scanned over 10,000 documents for cyberspace threats on Army web pages, while our education and leader outreach reduced the number of cross domain violations by 50 percent. Additionally, through a comprehensive approach, and implementation of a wide range of initiatives we increased the security of the Army Knowledge Online (AKO) website.

We continue to implement and leverage the capabilities of Host Based Security System (HBSS) on Army computers to better protect the individual at the end point system, and supports consistent implementation of DOD security policy on all computers. HBSS is critical to maintaining network security, and addresses current network vulnerabilities to prevent intrusions.

Knowing what's happening across all Army networks is vital to the Army's cyber ability to operate and defend our networks. While our asset visibility is increasing, our need for increased situation awareness and a common operating picture (COP) is essential. Fed by real-time network systems data and indications and warnings, an effective COP would allow us to act, react, and counteract at network speed, while conducting informed active defense operations. We continue collaboration with USCC, NSA, and key partners to unify research efforts and combine operational data with intelligence on Army systems to increase our cyberspace situational awareness.

The Army Cyber Defense in Depth strategy (Active Defense) facilitates a clear identification and prioritization of key cyber terrain, including physical and logical infrastructure and mission data. The strategy employs three overarching strategic objectives to protect key cyber terrain: Protect, including Defense of the Global Information Grid Operations (DGO) and Information Assurance (IA) measures; Defend, including passive Defensive Cyber Operations (DCO) organized around the deployment of perimeter and key terrain focused sensors, firewalls, and various host-based security systems and programs; Hunt, consisting primarily of active DCO utilizing advanced “active” sensors and rapid response actions. We continue to increase our capacity and capability to conduct each objective and our efforts will remain synchronized with the transition to the DOD Joint Information Environment (JIE).

Title 10 Responsibilities to Organize, Train, and Equip for Cyberspace Ops

As the Army’s service component to USCC, Army Cyber Command exercises the designated command and control authority and responsibility over trained and ready Army forces, as delegated by the Secretary of the Army and the Commander, USCC in support of his global mission. Additionally, Army Cyber Command, when directed, will serve as Joint Force Cyber Component Commander/Joint Task Force-Cyber.

Organized for today and moving to the future

Army Cyber Command is organized as the Army’s single operational level force with the major functions required to conduct our stated mission. Daily, we provide trained and ready forces to USCC support the execution of their mission. We have completed a wide range of work and continue to pursue other initiatives to better train, organize and equip the Army to conduct operations in cyberspace today and in the future. We are nested with the USCC mission and their three lines of operation--operate and sustain DOD information networks, defensive and offensive cyber operations. The command remains focused on providing an Army cyber force capable of meeting USCC and combatant commanders’ requirements in support of national and operational objectives, and in support of Unified Land Operations, to ensure U.S./Allied freedom of action in cyberspace.

Unity of effort and unity of command is essential in the cyberspace domain. Since activating the command, other organizations have been placed under the operational control of Army Cyber Command. The Army’s Network Operations Security Centers and our Regional Computer Emergency Response Teams are now part of the command, increasing the unity of command for the operation and defense of our networks. Additionally, Reserve Component cyber and information operations organizations are now under our operational control.

The most significant organizational milestone occurred on December 1, 2011 when the Army activated its first dedicated cyber brigade at Fort Meade, Maryland. The 780th Military Intelligence Brigade (780th MI BDE) (Cyber) is organized to support USCC and combatant command cyberspace operations. Army Cyber Command has operational control of the brigade. This brigade conducts signals intelligence and computer network operations, and enables Dynamic Computer Network Defense of Army and Department of Defense networks. When fully staffed, the 780th MI BDE will have more than 1,200 assigned Soldiers and civilian employees.

Additionally, Army Cyber Command is organized to provide dedicated information operations (IO) and cyberspace integration support to the Army and other Military Forces through the 1st IO Command and mobilized forces resident in the four Reserve Component Theater Information Operations Groups. These organizations deploy IO and cyberspace support teams; provides IO and cyberspace planning, analysis and technical reach back; and offers specialized IO and cyberspace training to assist the warfighter in garrison, during exercises, or in conflict. This support includes conducting IO and cyberspace operations planning, preparation, execution and assessment of the information environment; identifying IO and cyberspace vulnerabilities; leveraging IO and cyberspace intelligence analysis; and conducting training in IO and cyberspace operations to improve a unit's ability to successfully operate throughout the information environment. We have organized and deployed support teams to provide IO support to numerous Overseas Contingency Operations, exercises, and operations worldwide. We have also trained over 1,600 students in multiple information operations and cyberspace courses.

Army Cyber Command's robust and active involvement in assessments, wargames, and exercises with USCC, other combatant commands, and the Army, coupled with the results of the Training and Doctrine Command (TRADOC) *Cyber/Electromagnetic Capability Based Assessment* identified gaps in our ability to conduct cyberspace operations. In FY14, we will increase our capacity and address the following gaps: increase our World Class Cyber Opposition Force (WCCO) capacity to provide realistic, challenging cyberspace training in the conduct of Unified Land Operations to exercises, Home Station Training, and Combat Training Centers; increase our capability to conduct active defense of Army Networks through "Hunt Teams" that can find, fix, and mitigate currently un-detected malicious actors already inside the DoD infrastructure; provide capability to integrate cyberspace operations into Regional Army Land operations to support commanders' tactical and operational cyber planning and integration; increase intelligence personnel to support Army Cyber Command's operations Center, and improve our capability for rapid development of network defense tools; increase capacity to conduct our ability to conduct force modernization for cyberspace operations by developing requirements and solutions.

Army Cyber Command is working with the Reserve Component to identify capability gaps in support of Army Cyberspace Operations. Reserve forces will play a critical role in cyberspace operations for Homeland Security and defense of critical infrastructure.

Training for today and tomorrow

Strong training, leader development, and education programs are critical to operating in the cyberspace domain. This requires robust individual and collective programs to protect the force, conduct cyberspace operations and ensure mission accomplishment.

Everyone must increase their basic cyber awareness and the Army continues to conduct training to better protect our people from cyberspace threats. Army Soldiers, leaders and commanders must increase their understanding of cyberspace threats, vulnerabilities, and capabilities. Leaders must understand the operational impact, the risk and what they must do to mitigate their risk to ensure they maintain the freedom to operate in cyberspace and are able to leverage cyberspace to help achieve their objectives. We continue to increase cyberspace operations training in key Army leader education programs. As the cyberspace operations doctrine continues to develop, we will adjust our leader development programs.

In support of collective training and to prepare commanders and units for the cyberspace challenges they will operate in, we established and are employing a World Class Cyber Opposing Force (WCCO) at the National Training Center and in support of COCOM exercises. This realistic training allows commanders to see if they can defend against threats attempting to penetrate their network and increase their ability to operate in a contested and degraded cyberspace environment.

Our integration with USCC and sister service cyberspace components in support of exercises is robust. Army Cyber Command has doubled their participation in USCC, combatant command, and service exercises each year. We will integrate cyberspace operations into 13 Joint and Army exercises this FY, and will double that number next year. In addition to the WCCO we are providing Expeditionary Cyber Support Elements to combatant command and Army exercises, in order for commanders to plan, integrate and conduct cyberspace operations, with their operations.

As the Army finalizes Army Training Strategy 2013, training to conduct cyberspace operations will be a key component, to ensure we train as we fight. The training support system requires an integrated training environment with the right mix of live, virtual, and constructive capabilities to enable realistic cyberspace training to meet commander's training objectives.

Equipping to Conduct Cyberspace Operations

The Army has a wide range of capabilities being leveraged everyday to operate, defend and support offensive operations. We continue to respond to USCC and combatant commanders' requirements and have rapidly produced capabilities to support missions.

In order to attain and maintain cyberspace superiority, it is essential that we maintain an agile and responsive cyberspace acquisition process to provide required materiel solutions to operational requirements that keep up with the speed of change and stay ahead of potential threats.

Our research and development efforts are nested with DOD science and technology priorities, and we're working with key elements of Army Materiel Command, Defense Advanced Research Project Agency (DARPA), Federally Funded Research and Development Centers (FFRDC), and industry partners to provide a wide range of capabilities that assure effective missions, provide resilient infrastructure, support agile cyberspace operations, and are built on foundations of trust. Increasing our situation awareness and developing a defensible architecture that serves as an operational platform to the tactical edge for cyberspace operations are key efforts.

Through Network Integration Events (NIE) coupled with the Brigade Modernization Command (BMC) at Ft Bliss, the Army is fundamentally changing how it develops, tests and delivers networked capability to its operating force. This provides an opportunity to address capability gaps and insert new technologies into a robust operational environment to ensure they perform as required and create no cyberspace vulnerabilities.

The critical effort is to achieve a Joint Information Environment which provides a defensible architecture and an operational platform that enhances our ability to conduct cyberspace operations.

Recruit, Develop, and Retain a Cadre of Cyber Professionals

While technology plays an important role in the cyberspace domain, it is not technology that will win on the 21st Century's cyberspace battlefields. A team of elite, precise, trusted, and disciplined cyberspace professionals able to quickly act across the full range of mission sets is who will make the difference.

To meet today's and tomorrow's threats, we must recruit, develop and retain skilled, professional Soldiers (active duty and reserve component), Civilians and contractors who can meet future challenges and dominate the cyberspace terrain. However, our success requires a

highly skilled technical workforce that both government and private industry are competing for. We need to create a deeper national pool, while we develop the cyber skills we need now.

The Army's Military Intelligence (MI) and Signal Center (SC) Centers of Excellence (COE) are in the process of creating and revising skills that will better develop our cyber force to conduct cyberspace operations. In concert with this, they are reviewing and providing incentives, updating career development opportunity, and pursuing ways to retain these key skills.

The Army has created the 255S (Information Protection) Warrant Officer MOS. This specialty has been approved and trained warrant officers are now entering the Army inventory. We have also created the 35Q, Cryptological Network Warfare Specialist, and recruitment of Soldiers with a variety of incentives will begin this October. Additionally we have created new Additional Skill Identifiers for key cyber areas and are working to implement concepts for the development of new Areas of Concentration (AOC) focusing on Cyberspace Networks Integration as well as efforts to consolidate network engineering and information systems functional areas. A new enlisted MOS 25D, Cyber Network Defender, will be created and will start at the rank of Staff Sergeant.

Army Cyber Command Initiatives

Operational Planning and Critical Infrastructure Protection

Integrating cyberspace operations into planning is vital. Army Cyber Command planners and analysts are providing cyberspace operations planning and targeting support to USCC and Combatant Commanders to accomplish operational cyberspace effects. We're working to incorporate cyberspace and information capabilities into all contingency and crisis action plans. A key initiative includes leveraging existing plans developed by Headquarters, Department of the Army under their Force Protection and Antiterrorism Programs. We've built cyberspace operations into the Army's Critical Infrastructure Risk Management Program with the objective of identifying, assessing and reducing risk to the Army's critical assets beyond the conventional 'guns, gates and guards' approach. We're working with the Corps of Engineers to provide them the requisite cyberspace expertise to improve protection of their critical civil works infrastructure. Additionally, we're engaged in collaboration with Army Materiel Command and Installation Management Command to increase the security posture of Army owned Industrial Control Systems and Supervisory Control and Data Acquisition systems on Army installations.

Building Partner Capacity

We're building relationships with key allies and partner nations through operational planning and Theater Security Cooperation efforts, and supporting the development of combatant command and Army Service Component Command plans worldwide. We've completed our Theater Security Cooperation Strategy, which focuses on building partner capacity, enabling stability and security in the future cyberspace environment. By forging strong relationships with a variety of partners we are strengthening our collective cyberspace security and improving interoperability. Working closely with our allies and partners will promote better collective self-defense and present a collective deterrence while enabling the U.S. military to extend its ability to defend the Nation at home and abroad.

Building a Constellation of Cyberspace Partners

Army Cyber Command is leveraging existing Army processes to enhance a network of government, academia and industry partners with expertise in cyberspace. We are working closely with the United States Military Academy, Army Research Lab, and other partners to leverage intellectual capital and address our most significant challenges. We have also increased our investment in internships and fellowships, in scholarships with opportunities for advanced degrees, and in training with industry. Also, we are developing outreach programs through Science Technology Engineering Math (STEM) vehicles with academia.

Conclusion

For a command built around technology, it's important to understand people are Army Cyber Command's most valuable asset. Cyberspace operations require a world-class cyberspace force able to operate effectively today and in the future. Developing a robust cadre of cyber warriors is a top priority to ensure we maintain the advantage in the highly contested cyberspace domain.

Army Cyber Command has made great progress and will continue to remain trained and ready to ensure our forces maintain our freedom to operate. We're focused on providing a professional team of elite, trusted, precise, disciplined cyber warriors who defend our networks, provide dominant effects in and through cyberspace, enable mission command, and ensure a decisive global advantage. We provide depth and versatility in cyberspace to the joint force, and with our cyberspace capability we're providing options and flexibility for commanders and national decision makers to ensure the Army remains America's Force of Decisive Action, and Army Cyber Command remains, "SECOND TO NONE".