RECORD VERSION

STATEMENT BY

LIEUTENANT GENERAL EDWARD C. CARDON
COMMANDING GENERAL
U.S. ARMY CYBER COMMAND AND SECOND ARMY

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

OPERATIONALIZING CYBERSPACE FOR THE SERVICES

FIRST SESSION 114TH CONGRESS

MARCH 4, 2015

NOT FOR PUBLICATION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

Introduction

Chairman Wilson, Ranking Member Langevin, and Members of the Subcommittee, thank you for your support of our Soldiers and Civilians, our Army, and our efforts to operationalize cyberspace. It is an honor to address this subcommittee on behalf of the dedicated Soldiers and Army Civilians of U.S. Army Cyber Command (ARCYBER) and Second Army who work every day supporting Joint and Army commanders defending the Nation in cyberspace.

Army Cyber Command and Second Army have gained tremendous momentum building the Army's cyberspace capabilities and capacity. While making significant strides over the past two years, continued progress requires persistent congressional support in three core areas: people, operations, and technology. Put differently, we require resources, appropriate authorities, organizations, and capabilities, which can be synchronized in time and space with singular purpose to accomplish directed missions. This testimony focuses on the actions and activities the Army has underway, or is planning, to support our Title 10 responsibilities to organize, man, train, and equip Army cyber forces for cyberspace.

Mission and Organization

Army Cyber Command and Second Army directs and conducts cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace, and to deny the same to our adversaries. To accomplish this mission, the Secretary of the Army and the Army Chief of Staff streamlined the Army's cyberspace command and control structures by placing operational control of all Army operational cyber forces under one commander. The ARCYBER commanding general is responsible for Army and joint cyberspace operations; and is also designated as the Second Army commanding general responsible for all Army network operations (to meet United States Code Titles 40 and 44 requirements as defined by Headquarters, Department of the Army); and is also designated as the Joint Force Headquarters-Cyber (JFHQ-Cyber) commander responsible for cyberspace operations supporting select geographic combatant commands as directed by U.S. Cyber Command (USCYBERCOM). This construct works to enable unity of effort for cyberspace operations. The Secretary of Defense's recent decision to establish Joint Force

Headquarters- Department of Defense Information Networks (DoDIN) better aligned DoDIN operations, and by extension, Army networks, in a joint construct. This decision is essential to realizing the Department's goal of establishing one joint global network that connects Service networks as required for operational missions.

To achieve greater synergy and efficiencies within the Army, we have already established the initial elements of JFHQ-Cyber at Fort Gordon, Georgia, and will collocate the ARCYBER headquarters alongside National Security Agency-Georgia at Fort Gordon by 2020. Army Cyber Command is grateful that the FY16 President's Budget included $90 Million to build a state-of-the-art headquarters and operations facility at Fort Gordon.

Other recent Army decisions include the formation of the Army Cyber Institute at the U.S. Military Academy, West Point, the establishment of the Cyber Center of Excellence (Cyber CoE) at Fort Gordon, Georgia and the transition of the proponent for cyberspace operations from ARCYBER to the Army's Training and Doctrine Command at the Cyber CoE. The Cyber CoE is now the center of gravity for institutionalizing cyberspace, to include the necessary doctrinal, organizational, training, and materiel activities and policies, but it needs more dedicated resources to reach its full potential. The Cyber CoE will also integrate the electronic warfare and cyberspace operations proponents. As a partial solution and in accordance with the Total Army policy with reference to cyberspace, the Cyber CoE is initiating a partnership with the Army National Guard Professional Education Center in Little Rock, Arkansas to increase Cyber training throughput. These decisions have garnered operational and institutional momentum for cyberspace operations across the Army.

Bounding the Impact of Cyberspace on Military Operations

The Army's doctrine, Unified Land Operations, and recently published Army Operating Concept, establish a set of assumptions about conditions of the network and cyber-electromagnetic environment in which our forces are expected to operate. Services and combatant commanders base their plans on the expected Army capabilities, derived from this doctrine. As the current force downsizes, the Army must incorporate additional capability sets to amplify our units' means to operate more effectively in and through cyberspace.

For cyberspace, commanders at all levels will synchronize cyberspace operations into traditional land, sea, air and space activities in time and space and they will simultaneously maneuver with and through networked assets, the electromagnetic spectrum, and kinetic forces in mutually supporting operational constructs to achieve a disproportionate advantage. Achieving operational success also hinges on having the requisite command and control, alignment of authorities with missions, and other key enabling capabilities such as intelligence, information technology and communication activities. Tactical and enterprise networks are converging and future networks and the data they carry will be more contested and challenged — especially in the event of more intense forms of conflict.

The network is a critical enabler and operational capability for cyberspace operations. Congress, recognizing the importance of efficient and effective Information Technology (IT) and Information Assurance (IA) practices, legislated policy standards for both issues in Titles 40 and 44. Information Assurance, now known as Cybersecurity, has evolved into an operational imperative. Army Cyber Command is charged to plan and direct cyberspace operations in support of both Army and USCYBERCOM, and these missions require unity of effort and unity of command.

Now that cybersecurity has to be considered an element of cyberspace operations, where does cybersecurity fit, within the DoD's full-spectrum of cyberspace operations? In other words, where does statutory responsibility for cybersecurity nest with the operational commanders' responsibility to conduct full-spectrum cyberspace operations?

In response to congressional direction, DoD has recently created a new policy position within the Office of the Secretary of Defense, called the Principal Cyber Advisor, to bring an operational focus to all DoD activities affecting cyberspace. In the process, DoD clarified the policy role of the Chief Information Officer (CIO) function within DoD. The policy role of a CIO and the operational focus of a cyberspace operations commander must be mutually supportive to achieve statutory IT and cybersecurity (formerly Information Assurance) mandates. At the same time, operational commanders must assure the effectiveness of DoD networks as warfighting platforms and enablers of DoD operations.

Army leaders and cyber organizations must be capable of ensuring both freedom of maneuver in cyberspace, and integrating interactions between cyberspace operations and our traditional military activities, that are increasingly reliant on networks and network-dependent enablers. This requires an agile and adaptive network that does not exist in the Army today. The Army recognizes it must collapse its vast array of disparate networks, enclaves, and nodes at both tactical and enterprise levels to improve security, effectiveness and efficiency through network modernization. In his recent testimony, the Army's Chief Information Officer, LTG Robert Ferrell, described how the Army will address this issue.

Recruiting, Retaining and Maintaining Cyberspace Operations Personnel

The Army's first priority is to grow the Cyber Mission Force (CMF). We have grown its capacity exponentially since September 2013 with 25 of 41 teams at initial operating capability. We are on track to have all 41 CMF teams established and operating by the end of FY 16. However, they will not all be fully operationally capable until FY17.

Nothing is more important and vital to the growth of cyber capabilities than our ability to attract and retain the best people. As such, the Army views people as the centerpiece to cyberspace characterized by high degrees of competence and character. After a detailed study, the Army determined it needs 3,806 military and civilian personnel with core cyber skills. The Secretary of the Army established a cyber branch on September 1, 2014, and discussions are ongoing to determine how to better manage civilians supporting cyberspace operations. In addition, the Army has also created an "E4" additional skill identifier to better track personnel who have served in cyber and cyber related assignments as we build the branch and the force.

The Army has enjoyed success with in-Service recruiting into the growing cyber force, and is actively working to expand access to high-quality recruits. We have increased recruiting aptitude scores, visibly expanded our marketing efforts, and started work on a Cyber CoE-led initiative to encourage Science Technology Engineering and Mathematics cadets from both United States Military Academy (USMA) and the Reserve Officers' Training Corps (ROTC). We will commission the first 30 Cyber branch officers from both USMA and ROTC programs this summer. Once assessed

into the cyber branch, officers are managed by the U.S. Army Human Resources Command's Cyber Management Branch.

The Cyber CoE, in collaboration with ARCYBER and other stakeholders is working to implement a cyber Career Management Field for enlisted personnel that will encompass accessions, career management, and retention this fiscal year. The Army recently approved Special Duty Assignment Pay, Assignment Incentive Pay, and bonuses for Soldiers serving in operational cyber assignments. We have also expanded cyber educational programs, including training with industry, fellowships, civilian graduate education, and utilization of inter-service education programs (e.g., Air Force Institute of Technology and the Naval Postgraduate School). We are confident these will serve as additional incentives to retain the best personnel for this highly technical field.

Additionally, as part of our Total Force efforts, we have worked with the Reserve Components on key retention initiatives, including bonuses for critical skill Service members transitioning from active duty service into the Reserve Components; and accession bonuses for commissioned and warrant officers upon award of their duty qualifying military occupational specialties. Appropriate Special Duty and Assignment Incentive Pays should be considered for each of the Reserve Components' cyber Soldiers.

Recruiting and retaining Army Civilian cyber talent is challenging given internal federal employment constraints regarding compensation and a comparatively slow hiring process. Current efforts to attract and retain top civilian talent include extensive marketing efforts, and leveraging existing programs and initiatives run by the National Security Agency, Office of Personnel Management, and National Science Foundation.

The targeted and enhanced use of recruiting, relocation and retention bonuses, and repayment of student loans will improve efforts to attract, develop and retain an effective cyber civilian workforce. These authorities exist but require consistent and predictable long-term funding. Retaining highly skilled cyber professionals will continue to be a significant challenge that needs to be addressed.

Training

Training is critical to building and retaining our cyberspace force. Individual and collective cyber training has four components: training the CMF; integration of cyber into

unified land operations at echelon; training other cyber forces and enablers; and training to achieve basic cybersecurity awareness across the Total Army.

The Department of Defense provided resources to fund joint training requirements through USCYBERCOM for the CMF build for all the Services through FY16. This training allotment was only for Active Component Soldiers and Civilians. Training and sustainment resourcing after FY16 will become a Service responsibility, which the Army must fund beginning in 2017. The Army Cyber CoE recently conducted a Joint Cyber Training Forum in conjunction with USCYBERCOM and representatives from other Services and agencies to determine the way ahead for the transition to Service responsibility. The forum established that the Services are best positioned to develop the common core individual training and will re-evaluate the feeder school training model with regards to specific CMF operator work roles.

Both ARCYBER and the Cyber CoE are developing robust collective training methods that include both simulated, virtual, and real-world operational events on ranges and production networks that stress individual and team capabilities. We now require dedicated training facilities, support infrastructure and cyberspace live fire facilities consistent with joint range requirements at the Service and joint levels. These persistent training environments with dedicated facilities and resources will enable training innovations and further growth in capability and capacity available to combatant and Army commanders.

Army Cyber Command works closely with Army Training and Doctrine Command to ensure the continuum of cyberspace leader development, education, and training remains current and relevant despite the high rates of technological change. The Cyber CoE is explicitly charged with incorporating joint standards into existing programs of instruction in Military Occupational Specialty schools and the Combined Arms Center is incorporating cyber operations planning into their training scenarios. The Army must place equal attention toward the training of our cyber network defense service providers, our computer emergency response teams, and our information technology professionals. Finally, we must continue to improve the effectiveness of training on user practices for the Total Army. This also requires a culture change.

To ensure synergy between Army and joint training, the Army fully participates in the design and conduct of USCYBERCOM-sponsored and executed training and

exercise events. Army Cyber Command has also incorporated cyberspace operations into multiple operational plans and major exercises — building a cadre of cyberspace planners now supporting the joint force and Army commanders. The Army recognizes that cyber capabilities should also extend and be executed at the tactical edge to provide our forces a winning advantage across warfighting functions; therefore, the Army is working hard to define cyber requirements, including training requirements, for cyber support to our Corps and below formations with pilot programs planned for this year. We continue to expand our professional cyberspace opposing force, to more effectively train organizations and individuals on how to better protect and defend themselves against cyber attacks and how to operate in a degraded cyberspace environment during operational training events, such as major exercises and training center rotations.

Reserve Components Integration

Army Cyber Command is a total multi-component force of Active and Reserve Components which are fully integrated into the cyberspace force mix. Building the U.S. Army Reserve (USAR) and Army National Guard (ARNG) cyber forces is a high priority for the Army and ARCYBER. Our Reserve Components integration strategy was reflected in the Army's response to Section 933 of the FY14 National Defense Authorization Act, titled "Cyber Mission Analysis for Cyber Operations of the Department of Defense," which requested an analysis of the Reserve Components' role in cyberspace operations and is focused along several lines of effort, including: building an operational reserve in the USAR and ARNG for cyberspace crisis response; seeking opportunities to provide dual-use capability in support of Military and Homeland Defense and Defense Support of Civil Authorities missions; organizing cyber units to match CMF structure; aligning ARNG and USAR cyber forces under ARCYBER training and readiness authority; leveraging industry connected skills and using the Reserve Components' retention advantages for the Total Force.

The Army and ARCYBER will create a Total multi-component Army cyber force that includes 21 Reserve Component Cyber Protection Teams trained to the same standards as the Active Component cyber force. The civilian acquired skills and experience of Reserve Component Soldiers should be leveraged to provide equivalency for cyber training, enabling faster integration of the Reserve Components' capability into

the cyberspace force mix. In October 2014, in coordination with the Director of the Army National Guard, the Army activated one Army National Guard Cyber Protection Team in a Title 10 status supporting ARCYBER and Second Army.

Army Guard and Reserve forces routinely augment our headquarters now for cyberspace operations even as we work to build additional capability and capacity in the Guard and Reserve. Our Reserve Components' contributions include supporting Operation ENDURING FREEDOM, current operations in Southwest Asia, the Defense Information Systems Agency, USCYBERCOM, the standup of JFHQ-Cyber, and the defense of Army networks. As we move forward with the ARNG and USAR to build the Total Army cyber force, we will continue to train and integrate 429 ARNG and 469 USAR Soldiers into the Army's cyberspace operations.

Authorities are a complex problem. While the 933 report was an excellent start for defining the critical role our Reserve Components must play in cyberspace operations, authorities remain a challenge. While Title 10 authorities are clear, Title 32 and State active duty require the application of varied State constitutional, legislative, and executive authorities and coordination with state agencies and officials. While every State is different, there is merit in developing a common approach for authorities and capabilities to facilitate rapid and effective response in cyberspace.

Equipping the Army's Cyberspace Operations Force

As cyberspace grows more complex, and increasingly contested with sophisticated threats able to exploit known and unknown vulnerabilities, cyberspace operations and cybersecurity are exceptionally critical to national security. Sophisticated software is readily available that almost anyone can operate to achieve altruistic or nefarious ends. Aided by the proliferation of dual-use technologies, cyber actors of all types continue to exercise distinct advantages in cyberspace, especially when acting as an aggressor, as illustrated by the recent attacks on Sony Pictures Entertainment and Anthem health insurance. Electronic devices are increasingly embedded in everything from vehicles to guided missiles, and are often integrated into systems which are difficult and costly to update or upgrade as new threats or vulnerabilities are identified with increasing speed and widely ranging tempo. These factors represent malefactors impacting our warfighting systems.

In conjunction with our joint partners, the Army is aggressively improving its defensive posture beginning with architecture modernization efforts that reduce attack surface area, improve bandwidth and reliability, and fortify our long-standing but ever-critical perimeter defense capability. Notably, the Joint Regional Security Stack (JRSS) initiative, a component of the Joint Information Environment (JIE), will consolidate and improve the security of currently disparate networks, and provide foundational elements for enhanced situational awareness. Recent intrusions plainly underscore the extent to which DoD lacks sufficient situational awareness, putting operations and sensitive data at grave risk. With the proliferation of cyberspace capabilities globally, situational awareness also depends upon analysis of unprecedented quantities of data across friendly, enemy, and neutral space. Essential data elements are created throughout all phases of cyber attacks, which potentially originate deep within adversary space, and span our entire defense in depth. All of these separate data sources must be captured, aggregated, and correlated in near real-time to discover ever-evolving and diverse threats, including insider threats. Accordingly, we are aggressively pursuing foundational big data analytic capabilities required to deliver complete cyber situational awareness across all cyberspace operations. We have to modernize and get to the JIE as quickly as possible for improved mission effectiveness, enhanced security, and to increase efficiency — an imperative to protecting the DoDIN. Coupled with architecture modernization, these efforts align directly with JIE standards and its Single Security Architecture construct. In parallel, we are pursuing several advanced technologies to include network mapping, cloud and virtualization, and cyber infrastructure, platforms and tools, all of which are also fully integrated with USCYBERCOM's Unified Platform initiative. Additionally, we are also an active partner with Defense Advanced Research Projects Agency on its PLAN X cyberwarfare program that is developing foundational platforms for the planning and execution of cyber operations.

Given the pace of technological change, we must address distinct requirements, resourcing and acquisition processes. Together, they influence the entire spectrum of research, development, testing, evaluation, fielding, and sustainment. Dynamic and agile institutional processes are crucial to building and maintaining our decisive technological advantage. Recent updates to policy instructions for the Joint Capabilities Integration and Development System and the Defense Acquisition System provide a

foundation for requirements and acquisition governance and management rooted in agility, flexibility, and accountability with the objective to rapidly deliver cyberspace capabilities. The Army is also establishing the requisite fiscal structures and governance construct for investments and appropriations against urgent requirements. We must capitalize on the cumulative innovative power of industry, academia, and our National Laboratories to develop, test, and pilot promising technology and concepts. This requires a willingness to engage in iterative development and operations, for which success is measured by rapidly validating assumptions, failing cheaply, early, and often to ensure resources are liberated from non-performing programs and applied to those demonstrating promise, as well as delivering new or enhanced cyberspace capabilities in weeks or months instead of months or years.

In recognition of the unique demands of cyberspace, the Army has designated a cyber focal point at the office of the Assistant Secretary of the Army for Acquisition, Logistics, and Technology, and designated initial cyber materiel development roles across our Program Executive Offices. The Army is deeply focused on improving the security posture and resilience of its critical weapons and business platforms, ensuring cyber threats and vulnerabilities are considered both in the design phase and throughout production and sustainment. Remaining focused on DoD and USCYBERCOM guidance and directives we will ensure Army capabilities are presented in alignment with joint requirements and are interoperable within the joint community so that we optimize our collective investments across DoD. As we work to ensure current processes evolve to capitalize on innovative technologies, ultimately, new programming and acquisition authorities can provide greater flexibility to developing and fielding the infrastructure, platforms, and tools needed by our operational cyber forces.

Conclusion

Despite cyberspace operations' central role in current defense strategy, funding for core requirements remains uncertain. Cyber professionals – resourced with the right infrastructure, platforms and tools – are the key to dominance in cyberspace. Army Cyber Command, Second Army, and JFHQ-Cyber have made tremendous progress operationalizing cyberspace for the Army. Army networks are better defended and our cyber forces are better manned, trained and equipped. Recent institutional changes are helping recruit, retain, and continuously develop competent and disciplined cyber

professionals. This is a journey and congressional support is essential to ensure the Army has the required resources and authorities, and the right people, processes, and technologies to provide our combatant commanders and national decision makers with a ready, capable, and superior operational cyber force.

With your support, we can provide national leaders and military commanders with an expanded set of options in support of national security objectives. We will deliver.