RECORD VERSION

STATEMENT BY
LIEUTENANT GENERAL PAUL M. NAKASONE
COMMANDER, UNITED STATES ARMY CYBER COMMAND

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY
COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

SECOND SESSION, 115TH CONGRESS

ON SERVICES CYBER POSTURE

MARCH 13, 2018

NOT FOR PUBLICATION UNTIL RELEASED BY THE
COMMITTEE ON ARMED SERVICES

Chairman Rounds, Ranking Member Nelson, and Members of the Subcommittee, I want to thank you for your continued support of U.S. Army Cyber Command (ARCYBER) and our efforts operationalizing cyberspace for the Army in support of our warfighting commanders. It's an honor for me to represent the extraordinary Soldiers and Army Civilians of ARCYBER and the entire Army Cyber Enterprise. My testimony focuses on the Army's ongoing progress and key milestones the Army has reached since I last testified before this subcommittee in May 2017.

Army Cyber Command's mission is to direct and conduct integrated electronic warfare, information and cyberspace operations as authorized, or directed, to ensure freedom of action in and through cyberspace and the information environment, and to deny the same to our adversaries. Our operational units include: the Joint Force Headquarters-Cyber (Army); the Network Enterprise Technology Command (NETCOM); the 780th Military Intelligence Brigade (Cyber); the 1st Information Operations Command; and the Army Cyber Protection Brigade.

To be successful in our challenging mission, we closely partner with the other members of the Army Cyber Enterprise, which include the Army Cyber Center of Excellence (Cyber CoE); the Army Cyber Directorate within the Headquarters Department of the Army (DAMO-CY); and the Army Cyber Institute at West Point (ACI). Together, the Army Cyber Enterprise has made significant progress, operationally and institutionally, in preparing the Army for the future fight.

Operationally, ARCYBER achieved a significant milestone in September 2017 when all 41 Army Cyber Mission Force (CMF) teams became fully-operational, a year ahead of U.S. Cyber Command's (USCYBERCOM's) mandate. These teams were put on-mission as soon as they became available. In addition to these 41 active component teams, the Army is building 21 Reserve Component (RC) teams trained to the same Joint standards and integrated into a Total Force team. Last August, the first Army National Guard (ARNG) Cyber task force – Task Force Echo – assumed a critical mission for USCYBERCOM to engineer, install, operate, and maintain critical network infrastructure.

Today, the Army's Total Cyber Force is in the real-world fight 24/7—against near-peer adversaries, ISIS, and other global threats. Since last May, ARCYBER has provided support to Army commanders, with special emphasis on the Pacific theater, to ensure select networks, systems and data are protected and secure. Army cyber forces have also supported the Joint force as an integral part of Joint Task Force ARES (JTF-ARES), a JTF that I'm privileged to lead that has been countering ISIS' use of cyberspace as a domain to spread messages and coordinate combat activity. The work of JTF-ARES has been an important part of the coordinated multi-domain military campaign that helped defeat ISIS on the ground in Iraq and Syria.

Institutionally, the Army Cyber Center of Excellence has made significant progress developing the cyber workforce. In August, the first class of enlisted cyber operators graduated the Army Cyber School. The Cyber School is now training all Soldier cohorts (officers, warrant officers, and enlisted members) from all three force components (Active, Guard, and Reserve). The first Reserve Component Soldiers graduated from the Cyber School in FY17.

The Army invests approximately $1.9 billion annually to fund the cyber workforce, operational units, and operate and maintain the Army portion of the DoD information network (DoDIN). Investments into our cyber capabilities remain a top priority and we are continually refining our requirements, and improving resourcing and acquisition processes to ensure that they are agile enough to rapidly translate innovative concepts into realized capabilities.

Building on the Army's operational and institutional momentum, ARCYBER has pursued three mutually supported priorities: aggressively operate and defend our networks, data, and weapons systems; deliver effects against our adversaries; and design, build, and deliver integrated capabilities for the future fight. The following narrative describes the Army Cyberspace Enterprise's accomplishments across these priorities encompassing the areas of Operations, Readiness, Resources, Training, and Partnering.

Operations

Cyberspace operations encompass three interrelated mission areas: Department of Defense Information Network (DoDIN) operations, Defensive Cyberspace Operations (DCO), and Offensive Cyberspace Operations (OCO). Army DoDIN operations, which include building, operating, defending, and maintaining the Army's portion of the DoDIN, is our most complex mission because it underpins essential Army functions from mission command to business operations. Most cyberspace operations are defensive. Army Cyber Command's five Regional Cyber Centers (RCCs) provide enterprise-level defensive cyberspace operations and DoDIN Operations support to our Network Enterprise Centers, including local information technology services. We are currently standardizing our RCCs to ensure effective and efficient alignment of missions, tasks, manning, structure, and tools. Additional efforts to improve our network defense include "Bug Bounty" exercises and the Vulnerability Disclosure Program that partners us with industry to use the best ethical hackers to identify and fix previously unknown vulnerabilities in Army networks.

The 20 Cyber Protection Teams (CPTs) of our Army Cyber Protection Brigade (CPB) conduct active Defensive Cyberspace Operations and are invaluable in thwarting adversary actions that threaten critical Army and DoD networks and systems. Our CPTs deploy worldwide with mobile capabilities within hours of notification to protect and defend the Army's critical infrastructure, platforms, weapons systems, and data, supporting both national requirements and Joint and Army commanders.

Offensive Cyberspace Operations are cyberspace operations intended to project power by the application of force in or through cyberspace. The Army Cyber Mission Forces execute OCO using the same process of delegation of authority that governs conventional military combat operations, descending from the President, to the Secretary of Defense, to Combatant Commands and United States Cyber Command. The Army also has 21 OCO teams that are aligned in support of five Operational Commands: Cyber Command, Central Command, European Command, Pacific Command and Africa Command.

Readiness

Readiness is the Army's number one priority. Once Army Cyber Command (ARCYBER) completed the build of all 41 Army Active Component Cyber Mission Force (CMF) teams in September 2017, we transitioned from building cyber capacity to maintaining ready cyber forces. To do this, we are moving to a sustainable readiness model that will ensure our cyber forces are resilient and set conditions for multi-domain battle. Currently, we are investing $750 million into our Cyber Mission Forces.

To ensure our forces are ready to meet this challenge, the Army has funded a new cyberspace operations facility at Fort Gordon that will provide a cutting edge operational headquarters for both offensive and defensive operations. This facility is currently under construction, to be delivered in FY20.

In addition to the proper facilities, ready cyber forces also require a firing platform, operational infrastructure, and access. To address these needs, the Army has built a rapid capability development network, and has adopted an operational platform that Soldiers will use for training at the Cyber Center of Excellence and for operations upon graduation. Operational infrastructure provides the team's access to the cyberspace domain (Internet). A cyberspace capability is a device, computer program, or technique, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace. The cyberspace capability is what enables the operator to create effects in and through cyberspace targeting specified systems or devices. The ability of a trained cyber team to bring each of these technological capabilities to bear on a target is the true measure of readiness, and it is something that we are working every day to achieve.

ARCYBER is also working closely with the team developing the Persistent Cyber Training Environment (PCTE). When fielded, this system will provide an environment to train cyber operators both individually and collectively. The system will also be used to replicate various network environments that can be used to conduct mission rehearsals.

Sustainable readiness is not just focused on the Active component, it relies on the Total Army cyber force. The Army is building 21 Reserve Component (RC) Cyber Mission Force teams, including 10 U.S. Army Reserve (USAR) teams and 11 Army

National Guard (ARNG) teams, bringing the strength of the Total Army cyber force to 62 teams in total. These RC teams will be trained to the same Joint standard as the active duty force.

Over the last 10 months, we have made progress closing gaps in timing, resourcing, and mission alignment to ensure these Army teams are effectively integrated into the DoD Cyber Mission Force (CMF). The ARNG is scheduled to have one CPT reach Initial Operational Capability in FY18 and the USAR plans for two CPTs to reach Initial Operating Capability in FY18. The Cyber CoE continues to resource training for the RC teams, conducting transfer panels to transition existing Soldiers into the Cyber branch as well as allocating seats for training at the Cyber School. Once the teams are manned, they will be fielded the same equipment as Active component teams. All 21 Reserve Component CPTs will reach Initial Operating Capability by 30 September 2022 will be fully operational by 30 September 2024.

Network Readiness

Network readiness is a critical component of overall Army readiness. We invest approximately $400 million annually into network readiness. The Army currently measures network compliance with policy, regulation, and law through the Cybersecurity Scorecard, Command Cyber Readiness Inspections (CCRI), and Command Cyber Operational Readiness Inspections (CCORI). To assist Army units in improving their network readiness, ARCYBER conducts staff assistance visits prior to inspections. During 2017, every organization that received a staff assistance visit improved their scorecard measurement by an average of 15 points during the CCRI. The number of unit networks that failed to pass a CCRI dropped from 23 to three. Thus far, in 2018, we have had no failures. Additionally, ARCYBER has placed a renewed emphasis and commitment on the integration of the ARNG networks.

Making our networks more defensible is the main thrust of our priority to, “aggressively operate and defend our networks, data, and weapons systems,” designed to harden and modernize our networks and conduct defensive cyberspace operations. The Army is systematically improving its defensive posture with architecture modernization efforts that reduce attack surface area, improve bandwidth and reliability, and fortify our long-standing, but ever-critical perimeter defense capability.

A key priority has been upgrading Army computers to a more secure operating system, Windows 10 (WIN10). The Army recently achieved a major milestone with 95 percent of its approximately one million computers already upgraded. In order to stay ahead of the cyber threat, the Army is moving to an "as a service" approach for DoDIN services and capabilities, while maintaining operational oversight. These efforts include endpoint management and security, Army Enterprise Data Centers, and cloud services.

Endpoint management security, network convergence, and cyber analytics are enhancing our situational awareness, enabling us to see and defend DoD networks and giving us unprecedented levels of DODIN/Defensive Cyberspace Operations integration to better enable the warfighter while defeating cyber threats. Big Data analytics are foundational to improving cyber readiness and resiliency. The Army is using data analytics to improve our situational understanding of our networks—to see not only adversary activity, but also ourselves; and using this information as part of a risk management strategy to inform our cybersecurity decision making. The Army is developing an analytic framework for conducting advanced cyber defense that begins with continuous monitoring of the cyber operational environment.

We are also continuing modernization efforts designed to improve the Army's ability to defend its networks; achieve greater standardization and interoperability; and dispose of older, less secure systems. Network modernization efforts include: Joint Regional Security Stack (JRSS) migration, Multiprotocol Label Switching (MPLS) upgrades, and Installation Campus Area Network (ICAN) upgrades.

Network modernization efforts are also allowing us to increase bandwidth significantly, critical to moving toward a cloud-based and virtualized architecture. In the near future, the Army will use private, public, and hybrid clouds that will store and protect data in centralized repositories, improving data access and enabling global availability. As part of this effort, the Army is consolidating its data centers to enhance security and cost efficiencies. Reducing the Army's data center inventory will enable the follow-on transition to a long-term end state of four continental U.S. Army Enterprise Data Centers.

Additionally, as directed in the Section 1647 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 16, the Army's Cyberspace Operational Resiliency Assessment-Platform (CORA-P) program is evaluating the cyber vulnerabilities of major weapon systems. We are currently assessing 13 of 24 high priority systems. In response to Section 1650 of the NDAA for FY17, the Army is developing a plan to evaluate cyber vulnerabilities in the critical infrastructure of 27 Army installations.

Resources

The Army is on pace to man, train, and equip Total Army cyber forces to meet current and future threats. Readiness of the total force requires that our investments in cyber ensure that Active and Reserve forces are trained and equipped to common standards. People remain our most critical resource. Annually, ARCYBER spends $585 million to compensate its civilian workforce. Over the past 12 months we have devoted tremendous effort to ensure we can recruit, develop, employ and retain the talented workforce we need to accomplish our mission. We are also increasing our presence at key hiring fairs and participating in a number of existing internship programs. In addition, over the last three months we began exercising the direct hiring authority granted by Congress, which enables us to make on-the-spot tentative job offers at hiring fairs. All of these efforts should enable us to bring on hundreds of new civilian employees this year.

The Army has also begun conducting a Direct Commissioning pilot program, pursuant to the authority Congress gave us in Section 509 of the NDAA for FY17, which will commission civilians directly into the Army as 1st Lieutenants. To date, over one hundred people have applied for direct commissioning, though unfortunately most have been unqualified based on age, education or experience. There are currently two candidates who will likely attend initial training in May 2018. Initial indications from the first two iterations of the Direct Commissioning pilot are that legal limits on constructive credit for cyber officers are preventing more qualified candidates from applying for the program.

Since I last testified, the Army has expanded two key compensation programs for cyber soldiers. Assignment Incentive Pay (AIP) is designed to encourage officers, warrant officers and enlisted Soldiers to volunteer, train, and perform Cyber Mission Force work roles that are otherwise difficult to fill. Currently, ARCYBER has 1,850 eligible positions tied to AIP and the Army has budgeted approximately $1.6 million annually to compensate Soldiers who fill those roles.

Special Duty Assignment Pay (SDAP) is designed to compensate enlisted Soldiers assigned to duties designated as extremely difficult or that involve an unusual degree of military skill. Currently, ARCYBER has 1,245 eligible enlisted Soldier positions tied to SDAP and the Army has budgeted approximately $108k annually to compensate those Soldiers. Both programs will incentivize Soldiers for the unique talents and skill sets that are required to execute the Army's overall cyber mission, and improve the readiness of the Cyber Mission Force.

In addition to monetary compensation, the Army also offers cyber Soldiers the opportunity to participate in Training With Industry (TWI), or attend graduate school through the Advanced Civil Schooling program. ARCYBER also has the flexibility to detail some of our talented staff to the Defense Digital Service. These opportunities enable our Soldiers to learn from industry, improve their education, and address some of the Department's toughest technological problems.

ARCYBER Move to Fort Gordon, Georgia

Today, ARCYBER headquarters is split-based at Fort Belvoir, Virginia; Fort Meade, Maryland; and Fort Gordon, Georgia. Within four years, the ARCYBER headquarters will consolidate at Fort Gordon. As our Command transitions to Fort Gordon, the $180 million construction projects for our state-of-the-art headquarters is well underway, thanks to Congressional support. The new facilities will support more than 1,300 cyber Soldiers and civilian employees, and are projected to be ready for occupation in summer 2020. Army Cyber Command is expected to be fully operational at Fort Gordon by 2022. With the addition of the ARCYBER headquarters, the Augusta, Georgia region will become a center of gravity for U.S. Army cyberspace operations, providing a unified and consolidated operational and institutional home.

Limited Acquisition Authority

Following the establishment of USCYBERCOM and ARCYBER, both DoD and the Army recognized the need to find creative ways to maintain a competitive advantage in cyberspace. As it became apparent that speed and agility were critical in cyberspace, the Army needed to reduce the time and cost necessary to buy, test, and field new platforms and application technologies through the normal acquisition process. The Army subsequently initiated several innovative approaches designed to develop and deliver cyber capabilities more quickly, in order to keep ahead of our adversaries. This included granting ARCYBER Limited Acquisition Authority in August 2017, enabling us to meet the “need of speed” demanded in cyberspace operations. ARCYBER is using its Limited Acquisition Authority to wisely invest its resources in the most innovative and cutting-edge items that can rapidly benefit our force. We will likely leverage rapid contracting mechanisms such as Other Transaction Authority through partners like DIUx.

Training

The Army Cyber Center of Excellence (Cyber CoE) located at Fort Gordon, Georgia, provides training, force modernization, and career management for the Army’s Cyber, Signal, and Electronic Warfare specialties. The Signal School provides trained Soldiers to the operational force to conduct Department of Defense Information Network (DODIN) operations and cybersecurity. They train on average over 11,000 Soldiers per year across 17 Military Occupational Specialties. Signal Soldiers install, operate, and maintain the Army’s portion of the DODIN. The Signal School is aggressively pursuing a change to their training model that will provide all Signal Soldiers a common foundation in networking fundamentals in support of DODIN operations.

Established in 2014, the U.S. Army Cyber School trains Army Cyber Branch Soldiers and cyber personnel from the other Services. The Cyber School provides training in offensive cyberspace operations and defensive cyberspace operations at Fort Gordon, GA, and electronic warfare at Fort Sill, OK. The first class of Army Cyber

Branch lieutenants graduated in May 2016; the first class of cyber warrant officers graduated in March 2017; and the first class of new cyber enlisted recruits graduated in August 2017. Additionally, the Cyber School has trained 101 sister Service personnel and 68 Army Civilians. The Cyber School trained a total of 151 Cyber Branch Soldiers during FY16 and another 305 Soldiers during FY17. The Cyber School has established all courses necessary to meet anticipated training requirements for over 900 Soldiers annually to meet natural career progression and replacement of Cyber Branch Soldiers.

In addition to the Cyber School training, our Cyber Protection Brigade has developed "Cyber Gunnery Tables," similar in concept to the gunnery tables of maneuver branches, to ensure our Cyber Protection Team operators can effectively employ their DCO system. A Cyber Protection Team's DCO system enables the team to maneuver on Army networks to find, fix, and destroy enemy capabilities. These tables define the tasks that individuals, crews, and mission elements must master in order to effectively conduct DCO-Internal Defense Measures on the CPTs DCO system. They provide structured, methodical, and foundational training for individuals and teams. These gunnery tables also serve as training and readiness validation events, certifying that a crew has the required knowledge, skills, and abilities to participate in collective exercises as part of a mission element. They also provide a metrics-based assessment to objectively determine individual and crew readiness. Further, our teams use challenging competition-type exercises, such as Cyber Stakes, where individuals and teams can demonstrate their technical aptitude and sharpen their skills.

Additionally, the Cyber School is working several initiatives specifically directed at integrating Army Reserve Component (RC) cyber forces. For example, in FY17 the Cyber School conducted three Mobile Training Teams (MTTs) providing a total of 316 training seats; throughout FY18 they will conduct seven MTTs, and they are prepared to support a minimum of seven MTTs in FY19. These MTTs train approximately 30 students per iteration and are held at venues convenient to the Reserve Component units. The Cyber CoE has also conducted eight Cyber Branch Transfer/Reclassification panels and numerous off-cycle assessment panels for Reserve Component applicants, selecting 470 Soldiers from the Reserve Component for transfer into the cyber branch. The Cyber CoE is also working within the Army to ensure the Reserve Component can build personnel capacity and meet FOC training requirements without negatively impacting unit readiness reporting.

The Persistent Cyber Training Environment (PCTE) will provide high quality scenarios and event management to all four Services and USCYBERCOM, delivering a virtual environment that will enable training and mission rehearsals for squads, mission elements, and teams. The acquisition strategy for PCTE is to leverage existing infrastructure, transportation, and range resources, and to integrate the best government off-the-shelf and commercial off-the-shelf solutions. The program office is currently building cloud capacity that will host the Persistent Cyber Training Environment. Through incremental developments, the Army is creating low fidelity prototype training environments and leveraging the Service cyber components and DoD cyber ranges to develop high fidelity environments. Through a series of Cyber Innovation Challenges, two in progress to date, the program office will leverage industry and existing cyber training capabilities to refine event management and training management.

CSCB

Since 2015, the Army's Cyber Electro Magnetic Activities (CEMA) Support to Corps and Below (CSCB) pilot has been integrated into nine rotations at the Army's Combat Training Centers (CTCs), helping Brigade Combat Teams (BCTs) integrate CEMA, which spans offensive and defensive cyberspace, electronic warfare, and information operations into a BCT's operations process. This pilot has helped BCTs leverage CEMA to understand their unit's footprint in the cyberspace domain and in the electromagnetic spectrum, and to better deliver cyberspace effects and conduct electronic warfare in support of their operations. The pilot has also helped the BCTs to maximize the role of the organic Electronic Warfare Section and identified the best methods of leveraging the new Expeditionary CEMA Team concept under the proposed Cyberspace Warfare Support Battalion (CWSB).

The lessons learned through our CSCB initiative have been valuable and put to direct use. Today, our cyber forces are supporting operational units in Iraq, Syria, Afghanistan, Korea, and Europe. We're equipping and training units with new tools, giving them a marked advantage over the adversary. We're also supporting training for the new Security Force Assistance Brigade, providing expeditionary and remote OCO, DCO, Electronic Warfare, and Information Operations. ARCYBER is helping shape the CEMA capabilities of the Army's Multi-Domain Task Force initiative and lessons learned are being applied to global contingency operations. We continue to support the training of Brigade Combat Teams, helping build-out a contested and congested cyberspace domain and Electro Magnetic Spectrum infrastructure at Combat Training Centers and replicating real near-peer threats.

Partnering

In our headquarters we often say that cyber is a team sport. Since I last testified, we have partnered closely with the Defense Digital Service (DDS) on a number of important projects. We have worked closely with DDS to conduct a bug bounty on one of the Army's key logistics systems to identify and resolve vulnerabilities before our adversaries could find and exploit them. Additionally, we have partnered with them to pilot a new training program at the Cyber Center of Excellence for enlisted cyber Soldiers. The intent of this pilot program is to shorten the training time for recruits. If recruits demonstrate the necessary skills, they can proceed more quickly through the training program. This more dynamic training format would enable many of the recruits with a computer science background to complete what was a six-month training program in as little as 12 weeks.

We have also partnered with the DDS to create tiger teams composed of DDS personnel and ARCYBER Soldiers. One such team developed a counter-unmanned aircraft system (C-UAS) capability that can be used by battlefield commanders. Finally, Army Cyber Command has collaborated with DDS to develop an outpost at Fort Gordon, by the summer of 2018, which will facilitate identifying top technical talent to support the rapid development of solutions to top cyber threats.

Army Cyber Command is also closely partnered with Defense Innovation Unit – Experimental (DIUx). We meet monthly to share and collaborate on problem statements and commercial solutions that could address Army operational gaps and needs. Several projects sponsored by DIUx are under evaluation by ARCYBER for

Defensive and Offensive Cyber Operations capabilities. In particular, we are assessing specialized software as a solution to endpoint threat detection/interrogation. We have also coordinated with DIUx for problem statements relating to Advanced Sensors and Machine Learning.

Key partners and allies bring unique capabilities, skills and approaches to the cyberspace operational environment. Each nation has benefited from our partnerships through information sharing and operational collaboration. Maintaining and improving these relationships will be critical to operational success regardless of the potential adversary.

Conclusion

The Army Cyber Enterprise has made significant progress throughout 2017.

- The Army's 41 active Cyber Mission Force teams are fully operational, on-mission, and delivering unprecedented capabilities to our combatant and Army commanders every day.
- We are continuing to make our networks more secure and more defendable through modernization and consolidation.
- The Army Cyber Center of Excellence is now training all cohorts and all components, and preparing to integrate the Electronic Warfare force into the cyber career field.
- Construction on the Army Cyber headquarters complex at Fort Gordon, Georgia is taking shape, and will transform the Fort Gordon region into a cyberspace hub for the Army and the Nation.
- Our investments in Soldiers and Civilians through innovative talent management initiatives are paying off.

The Army is driving hard to lay the groundwork for the future force. We are moving toward developing a sustainable readiness model for the Total Army cyber force; building an in-house development capability; and organizing an expeditionary CEMA force. Every day our people are innovating and adapting, positively impacting the way we organize, train, and equip the Army cyber force, enabling us to stay ahead of our adversaries and to ensure the Army is ready to fight and win. With the continued support of Congress, the Army will continue to build upon this tremendous momentum to deliver an elite cyber force to our warfighting commanders.