THE INSTITUTE OF LAND WARFARE • AUSA

National Security Watch

NSW 14-1 5 May 2014

# The Army in Cyberspace

by Frank L. Turner II

> *Cyber has escalated from an issue of moderate concern to one of the most serious threats to our national security. We now live in a world of weaponized bits and bytes, where an entire country can be disrupted by the click of a mouse.*
>
> General Martin E. Dempsey[1]

## Introduction

America is immersed in cyberspace. Government, private enterprise and most individual American citizens enjoy the benefits and efficiencies of cyberspace. Wealth, intellectual property and reputation are just a small sample of the individual and collective riches that can reside within it. In fact, most average Americans would struggle to remember living without some of its conveniences. This phenomenon is not unique to America; it is pervasive around the world, among allies and adversaries of the United States alike. Innovation continues to expand the reach and utility of cyberspace, while also introducing new vulnerabilities.

National security experts remain bitterly divided about the role and importance of cyberspace in the next conflict. Some even fear there could be a cyber-Armageddon event looming just over the horizon. The nature of competition in cyberspace advances generates legitimate concerns that the United States may not always be prepared for a cyber "unknown-unknown," an undetectable advancement that provides others with an asymmetric cyber advantage. Cyberspace is like a game of global chess, wherein the players are unsure who else is playing, uncertain of friend or foe, unclear about the terrain and unconvinced the players will act according to established norms and rules.[2] Uncertainty in cyberspace makes it difficult to assess risk, which is determined by the probability of an event and the severity of its outcome.

Despite the lack of consensus on cyber risk, few can disagree that cyberspace has already become a hotly contested domain that will play a prominent role in the next conflict. Military operations in cyberspace offer great opportunities while simultaneously posing significant challenges. These potential vulnerabilities demand that the United States military continue to build a world-class cyber force.

## Describing Cyberspace

What seems like a simple task—describing cyberspace—is actually quite complicated. Even among cyberspace professionals, agreeing on what comprises cyberspace is difficult. The Department of Defense (DoD) defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[3] The concept of interdependence describes the links among the individual technologies that create it. Definitions are important in the military because of their role in shaping resource and responsibility decisions.

This series is published on an occasional basis by AUSA's **Institute of Land Warfare,** designed to provide news and analysis on pertinent national security issues to the members and leaders of the Association of the United States Army and to the larger policymaking community. The content may represent the personal opinions of the author(s) and not necessarily the position of the Army, the Association or its members. For further information, please visit the AUSA website at **www.ausa.org.** Reproduction and distribution of this document is encouraged.

A functional framework can also describe the interdependent components of cyberspace: people, data, software, hardware and infrastructure. People are at the core; ultimately, cyberspace is underpinned by the reliability and trust of the people. Individual and collective participation is continually influenced by dynamic risk–reward analyses. Data is the treasure and includes blogs, text messages, e-mail messages, tweets, chats, images, videos, stock quotes, bank account balances, financial transactions, Personally Identifiable Information (PII)[4] and intellectual property. Software is the lifeblood and describes the actual computer code, whether benevolent, benign or malicious. Hardware, the appendage, includes the array of user devices that access cyberspace. Infrastructure is the backbone and includes the cables, lines, towers and structures that link, transmit and store data. Learning about the components of cyberspace helps to understand and describe how and where new innovations may fit.

Using this functional framework, a digital camera can be described as hardware (with internal software) that allows people to capture data that can be uploaded and transferred via other hardware (with software) and shared across the infrastructure with other people. Another example is cloud computing. In traditional computing, users created and stored data on their hardware using productivity software. In cloud computing, users still create and access data from their hardware, but the data and productivity software reside on centralized infrastructure. This alternate approach aims to improve security, collaboration and productivity.

The following attributes and trends help describe the current nature of cyberspace:

- **People.** Cyberspace is individual and user-centric. Individual users decide when to access, what to access, whether to be an active (post) or passive (read) participant and ultimately what to believe. Social networks embody the empowerment and expression of the individual user. Recent studies classify more than one-third of the world's population as Internet users[5] and estimate there are approximately 8.7 billion devices connected to the Internet.[6]
- **Data.** Cyberspace is massive and growing. The physical size of the Internet (only part of cyberspace) is estimated at more than 1.74 billion webpages.[7] Data files (text, image, audio and video) have become larger and more sophisticated to generate the need for data warehouses and repositories. "Big data" is a term that describes the "tools, processes and procedures allowing an organization to create, manipulate and manage very large data sets and storage facilities."[8] Entities that manage big data well have an advantage over those who do not.
- **Software.** The attacker, who needs only to find a weakness in access architecture or vulnerability in computer code, currently has the advantage over the defender. The sheer number of attacks places cyber security professionals in a defensive posture. Cybercrime is also on the rise in both scope and frequency.
- **Hardware.** Cyberspace has a rapid rate of change. Most people working in cyberspace accept that the pace of change follows Moore's Law, which forecasted in 1965 that the number of transistors on an integrated circuit would double every two years.[9] This exponential change is common in many other areas of cyberspace, resulting in a disposable-technology culture where items rapidly become obsolete. Cyberspace is also increasingly mobile. The widespread proliferation of smartphones and tablets has transformed how people access cyberspace. The mobile trend was accelerated by the emergence of applications, or icon-based software, which numbered more than 1,000,000 at the Apple App Store alone as of October 2013.[10] Allied Business Intelligence Research forecasted that users would download 58 billion smartphone applications and 14 billion tablet applications in 2013.[11]
- **Infrastructure.** Cyberspace transcends borders. Cyber governance and policy remain underdeveloped. Although DoD, the Department of Homeland Security and the Federal Bureau of Investigation are assigned top-level domain responsibilities in the United States, their limited reach beyond the borders can create sanctuary and make attribution difficult. Every other nation-state has this challenge as well.

### The U.S. Army in Cyberspace

After more than 12 years of war, the United States wrestles with many difficult decisions in shaping the joint force for 2020 and beyond. The initial impact of sequestration on readiness and modernization has already proven ominous for the Army. The increasing importance of the cyber domain continues to introduce new opportunities and challenges as the Army prioritizes its limited resources among personnel, readiness and modernization requirements.

The Army has a long and storied history of innovation, experimentation and leadership within cyberspace. The decade-long Army transformation following Operation Desert Storm and the Army Task Force XXI Advanced Warfighting Experiment helped prioritize the acquisition and integration of cyber technologies that improved situational awareness, command and control and weapons precision. Innovation within the cyber domain remains significant as the Army charts the course to Force 2025.

Determining and emplacing the right proponent structure is vital to developing and managing new functions. The Army uses the DOTMLPF (Doctrine, Organization, Training, Materiel, Leader Development and Education, Personnel, Facilities) process within the Force Modernization Proponent System to meet its Title 10 responsibilities and manage strategic change.[12] Under the former proponent construct, there were several dispersed force modernization proponents in cyber and cyber-related areas throughout the Army generating force:

- Combined Arms Center – Army operational knowledge management, command and control (now called mission command), computer network operations (now called cyberspace operations), electronic warfare and information operations.
- Signal Center of Excellence – signal/communications networks and services.
- Chief Information Officer/G-6 – information management (which includes information technology, the Army Enterprise Portal and Army Enterprise Architecture and Infostructure); also provides oversight of DOTMPLF requirements, future capabilities developmental efforts and integration tasks of Army operational knowledge management and computer network operations for both Army and joint operations.[13]
- Provisional Cyber Branch – provides career management, development and readiness to the Army's cyber forces.[14]

The emergence of U.S. Army Cyber Command (ARCYBER) added more stakeholders to the DOTMLPF process. The Army DOTMPLF process can be arduous for one proponent to navigate, let alone build consensus among several proponents.

**The Army Proponent System**

Army Regulation (AR) 5-22, *Force Modernization Proponent System*, describes how the Army manages strategic-level change to meet many of its Title 10 responsibilities. The DOTMLPF (Doctrine, Organization, Training, Materiel, Leader Development and Education, Personnel, Facilities) process is the centerpiece. Headquarters, Department of the Army (HQDA) and Training and Doctrine Command (TRADOC) have significant duties and responsibilities within the Force Modernization Proponent System. Defined below are the three types of duties within the system:[15]

- Functional process owner – the HQDA principal official with primary responsibility for Army-wide management of one or more of the DOTMLPF processes.
- Force modernization proponent – the HQDA principal official or the commander, commandant, director or chief of a center, school, institution or agency with primary duties and responsibilities relative to DOTMLPF and related requirements for a particular function.
- Branch proponent – the commandant of a branch school or the chief of a branch of the Army that is responsible for leader development, training and recommendations on the personnel lifecycle appropriate for the branch.

The functional process is vertical, culminating with final decisions at HQDA. Both branch and force modernization proponents own the horizontal responsibilities for all of the DOTMLPF processes for assigned functions. TRADOC uses eight Centers of Excellence[16] and 32 Army schools to conduct many of its force modernization proponent responsibilities.[17] The chart on the following page defines the DOTMLPF terms and identifies the HQDA Functional Process Owner and the TRADOC Domain Lead (TRADOC's counterpart to the HQDA Functional Process Owner).

| Function | Definition<br>(AR 5-22) | HQDA Functional<br>Process Owner (AR 5-22) | TRADOC Domain Lead<br>(TRADOC 71-20)[18] |
|---|---|---|---|
| **Doctrine** | Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. | DCS, G-3/5/7<br>(Operations and Plans) | CG, Combined Arms Center<br>(CAC) |
| **Organization** | A unit or element with varied functions enabled by a structure through which individuals cooperate systematically to accomplish a common mission and directly provide or support warfighting capabilities. Subordinate units/ elements coordinate with other units/elements and, as a whole, enable the higher-level unit/ element to accomplish its mission. This includes the manpower (military, civilian and contractor support) required to operate, sustain and reconstitute warfighting capabilities. | DCS, G-3/5/7 | Army Capabilities Integration Center (ARCIC), Analysis & Integration Directorate (A&ID), Force Design Division (FDD) |
| **Training** | The instruction of personnel to increase their capacity to perform specific military functions and associated individual and collective tasks. | DCS, G-3/5/7 | CG, CAC |
| **Materiel** | All items (including ships, tanks, self-propelled weapons, aircraft and so forth, and related spares, repair parts and support equipment but excluding real property, installations and utilities) necessary to equip, operate, maintain and support military activities without distinction as to its application for administrative or combat purposes. | Army Acquisition Executive & Assistant Secretary, Acquisition, Logistics and Technology ASA(ALT) | ARCIC |
| **Leader Development and Education** | The product of a learning continuum that comprises training, experience, formal education, and continual self-improvement. | DCS, G-3/5/7 | CG, CAC |
| **Personnel** | The development of manpower and personnel plans, programs and policies necessary to man, support and sustain the Army. | DCS, G-1<br>(Personnel) | TRADOC DCS G-3/5/7, Leader Development Integration Directorate, Personnel Proponency Division |
| **Facilities** | Real property consisting of one or more of the following: a building, a structure, a utility system, pavement and underlying land. | Assistant Chief of Staff for Information Management | TRADOC G-1/4<br>(TRADOC Engineer) |

The future of a single Army cyber proponent is promising. In December 2013, the Army announced that ARCYBER will move to Fort Gordon, Georgia. Separately, TRADOC will establish the Cyber Center of Excellence there and consolidate cyber and network operations under one commander, which “creates institutional unity and provides a focal point for cyber doctrine and capabilities development, training and innovation.”[19] It is likely that the Cyber Center of Excellence will assume the majority of the dispersed horizontal DOTMLPF responsibilities, which in time will create efficiencies and improved capabilities. The special and unique relationship between ARCYBER and the Cyber Center of Excellence will create synergy between the cyber operating force and generating force and provide the Army a tremendous opportunity to quickly grow capabilities that have an institutional foundation. In the meantime, the Army continues to make improvements within the cyber domain. A review of some of the DOTMLPF highlights and challenges will provide a sense of where the Army is and where it is going in cyberspace.

## Doctrine

The development of suitable cyber doctrine is paramount to providing a shared understanding and establishing the scope and responsibilities with the cyber domain for the Army. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, notes that doctrine is "authoritative but requires judgment in application." Published in February 2014, Field Manual (FM) 3-38, *Cyber Electromagnetic Activities (CEMA)*, is a strong foundational document to provide guidance and direction for the Army's way forward in cyberspace. Important takeaways from the new cyber doctrine include:

- Commanders are responsible for CEMA. They must understand the CEMA functions, executive authorities and other legal considerations.
- Cyberspace operations are organized into three interdependent functions—offensive cyber operations, defensive cyber operations and Department of Defense information network operations.
- "Conduct CEMA" is one of the four staff tasks of the mission command warfighting function; it integrates and synchronizes cyber, electronic warfare and spectrum management operations.
- CEMA must be part of the operations process and must be integrated into the Military Decision Making Process, Intelligence Preparation of the Battlefield, targeting and risk management steps.
- Integration of CEMA with Unified Action Partners is challenging but necessary. Unified Action Partners may include joint, interagency, intergovernmental, multinational, nongovernmental organizational or private industry partners.[20]

As the cyber domain continues to develop and transform, Army doctrine must remain agile and continue to evolve. During the 2014 Association of the United States Army (AUSA) Winter Symposium, Lieutenant General Edward C. Cardon, the commanding general of U.S. Army Cyber Command, signaled a potential doctrinal way forward for cyberspace in his observation that the virtual tactics are parallel to the physical tactics of offense, defense and security. The volume of intellectual rigor committed to understanding the nature of cyberspace will provide depth and breadth for Army doctrine writers who will get it incrementally more right.

## Organization

The establishment of the new Cyber Mission Force (CMF) has augmented the Army's legacy cyber organization. Formerly comprising signal network operations units and military intelligence signal intelligence (SIGINT) units, Army cyber units now include formations designated against the three primary mission areas of United States Cyber Command—offensive cyber operations, defensive cyber operations and the operation and defense of the Department of Defense Information Networks (DoDIN)—that collectively provide full-spectrum virtual operations. The forthcoming establishment of the Cyber Center of Excellence will provide the Army with a focused, dedicated generating-force organization that is best postured to help the Army meet all of the Title 10 requirements inherent in a rapidly growing cyber operational force. A synopsis of the following cyber operating force units highlights the Army's organizational developments within cyberspace: U.S. Army Cyber Command, 1st Information Operations Command, 311th Signal Command, the 780th Military Intelligence Brigade and the forthcoming Cyber Protection Brigade. The important takeaway is that Army's cyber organizations are operating on the cutting edge.

Activated at Fort Belvoir, Virginia, in 2010, U.S. Army Cyber Command is an operational Army force assigned to U.S. Strategic Command. Designated as the Army Force Component Headquarters of U.S. Cyber Command (a sub-unified command of U.S. Strategic Command), ARCYBER reports directly to Headquarters, Department of the Army and is the primary Army headquarters responsible for cyberspace operations in support of joint requirements. ARCYBER is the single point of contact for reporting and assessments of incidents, events and operations in Army networks; they also synchronize and integrate the Army response.[21] The commander, dual-hatted as the commander of Second Army, will lead almost 21,000 Soldiers and civilians who ensure freedom of action in cyberspace for the U.S. military and its allies and deny the same to our adversaries.[22]

The 1st Information Operations Command (Land) (1st IOC) is the Army's premiere information operations organization. Several unique capabilities empower 1st IOC to conduct cyberspace operations support, computer emergency response and computer network operations planning and exercise support. 1st IOC also manages the

Computer Defense Assistance Program that conducts network assistance visits, network damage assessments and network penetration testing. Finally, the 2d Battalion, 1st IOC is designated as the Army's World-class Cyberspace Opposing Force; they are tasked to provide a formidable virtual adversary during training events and exercises, including rotations at the combat training centers.[23]

The 311th Signal Command (Theater) (311th SC), headquartered at Fort Shafter, Hawaii, is a theater enabling command of the U.S. Army Pacific Command. Comprised of the 1st Signal Brigade and the 516th Signal Brigade, the 311th SC has tactical-level and operational-level signal commands that are forward-based throughout the Pacific Theater. The 311th SC plans, builds, operates, defends and extends Army and joint networks to enable full-spectrum, unified land operations across all joint operational phases. The robust engagement and exercise strategy in the Pacific Theater allows the 311th SC to partner and train with a wide array of unified action partners, often in a disconnected, intermittent and low-bandwidth environment.[24]

The 780th Military Intelligence Brigade (Computer Network Operations) is one of the Army's most capable cyber units, with a lineage of operating as a cyber-network operations force since 1998. Headquartered at Fort Meade, Maryland (with one battalion at Fort Gordon, Georgia), the 780th Military Intelligence Brigade conducts signals intelligence; executes computer network operations; enables dynamic computer network defense; achieves operational effects in support of Army, combatant command and Department of Defense operations; and denies adversaries freedom of action in cyberspace.[25] During the 2013 AUSA Annual Meeting, the 780th Brigade commander, Colonel Jennifer Buckner, highlighted the brigade's Google-like atmosphere and unique approach to talent management as key to getting the most from her unit.[26]

The Army is standing up an elite Cyber Protection Brigade at Fort Gordon, Georgia. As the headquarters for all Army cyber protection teams (CPTs), the unit will conduct global cyberspace operations to deter, disrupt and defeat our adversaries. CPTs will "provide a comprehensive, dynamic cyber defense in-depth capability which provides a more proactive cyber defense posture with more sophisticated tools in the tool box, including greater coordination with military intelligence assets."[27] The Cyber Protection Brigade is actively recruiting highly qualified Soldiers, officers and Department of the Army civilians for positions as operators, analysts, planners and leaders who will aggressively defend Army networks on the front lines of cyberspace.

The Army will continue to grow cyber capabilities for the foreseeable future. The diverse experiences and lessons learned of U.S. Army Cyber Command, 1st Information Operations Command, 311th Signal Command, and the 780th Military Intelligence Brigade provide unique perspectives for improving cyber unit designs as the Army continues to develop tailorable and deployable cyber organizations.

## Training

Nearly everyone in the military works at least peripherally within the cyber domain and basic cyber skills are essential throughout the ranks. Different levels of cyber capabilities are required within the military based on the specific duties and responsibilities of Soldiers and leaders. LTG Cardon noted during the AUSA Winter Symposium that the Army probably needs to conduct a review to determine individual and collective tasks in cyberspace. This would allow the Army to develop a comprehensive training strategy for cyberspace.[28] The Cyber Center of Excellence should play a lead role in developing the strategy.

A cyber training strategy should address both the generalist and the specialist. The generalist does not hold a cyber-related military occupational specialty (MOS) and typically performs only basic tasks in cyberspace such as accessing the Internet, using productivity applications, corresponding via e-mail or operating one of the Army's automated mission command systems. The cyberspace specialist has a technical background in a cyber or cyber-related MOS. It takes two to three years to educate, train and develop an Army cyberspace specialist. The training is challenging and rigorous. It is noteworthy that the Army graduation rates in the joint cyber training program have improved from 40 percent to 80 percent.[29] Just as cyberspace is dynamic, the training strategy must be dynamic and evolve as the tasks, conditions and standards change.

A comprehensive training strategy will allow the Army to develop and employ its collective training resources more effectively. Virtual, constructive and gaming training will become increasingly important as defense budgets continue to contract. Virtual, constructive and gaming environments have the potential to provide lower-cost individual and collective training experiences. The Army has many virtual, constructive and gaming modules, but private industry still has much to offer in this area.

### Materiel

For the foreseeable future, the United States will remain engaged in a perpetual race for cyber capabilities that demands persistent investment to keep pace with peers, allies and adversaries. Today, the Army is more a taker than a maker of cyber innovation—and there is no shortage of new cyber technologies from the private sector or the cyber industrial base. A healthy balance of acquisition with science and technology in cyber will allow the Army to stay engaged with these kinds of innovations. Unfortunately, some of these necessary investments will be for evolutionary innovations with brief lifecycles before obsolescence. Investments in science and technology are oriented on harnessing innovations that produce leap-ahead, disruptive or paradigm-shifting revolutions. The Army's deliberate efforts, discussed below, leverage both the acquisition and the mature science and technology developments to modernize the network.

**Network Modernization.** LandWarNet (LWN) is the Army's new enterprise network that will empower the Soldier and the squad with the most accurate, relevant and up-to-date information required for unified land operations. LWN is designed as a single, secure, standards-based network environment. As a single network, LWN is split-based and accessible throughout an entire Army Force Generation cycle. Its Installation as a Docking Station (IAADS) capability will enable units to train on mission command systems, conduct live/virtual/constructive training and execute MOS-specific foundry training on the network. Network security remains a significant task for all cyberspace users. LWN capitalizes on the Joint Information Environment (JIE) framework to improve network security and efficiency through consolidation of information technology (IT) infrastructure, implementation of a cloud environment and incorporation of the enterprise directory and e-mail services to establish a single network identity for each user. The standards-based approach establishes accreditation requirements that reduce reliance on proprietary systems and ensure compatibility across systems; this helps streamline the cyber acquisition process and reduce costs.[30]

**Network Integration Evaluations.** In 2011, the Army conducted the first Network Integration Evaluation (NIE) to improve integration and performance of the network. The NIE is a two-to-four-week exercise conducted semi-annually that brings together the Army's requirement, resource and acquisition communities with the cyber industrial base to focus on a series of network integration and maturation objectives and priorities. The Brigade Modernization Command is responsible for the execution of the NIE. The 2d Brigade, 1st Armored Division (2/1AD) is the center of gravity for the NIE; 2/1AD conducts the training missions and certification events against opposing forces in challenging conditions. Their Soldiers provide the critical performance feedback that allows the Army to decide which capabilities to acquire. The approved capabilities are packaged and procured as capability sets that are fielded to deploying brigade combat teams. The latest capability sets feature Warfighter Information Network–Tactical (WIN-T) Increment 2, which provides mission command on the move with voice, video and data capabilities. NIE 14.2 is scheduled for April–May 2014.[31]

The Army's science and technology community is focused on what happens next. Annually, the Institute of Electrical and Electronics Engineers identifies the top ten technology trends for the upcoming year in the commercial sector. The following five from the 2014 list may provide some insight into where cyberspace may be heading: mobile cloud emerges; big data becomes extreme data; three-dimensional printing becomes more widespread; industry invests in next-generation infrastructure that improves mobile connectivity; and the balance shifts between identity and privacy on social networks.[32]

### Leader Development and Education

An Army leader development and education strategy for cyberspace must address both the generalist and the specialist. The strategy must also address cyber education, experience and self-development learning. We are living in an age where, generally speaking, the younger someone is, the more capable he or she is in cyberspace; special emphasis should be placed on the graduate and executive levels of the commissioned, warrant and noncommissioned officer professional military education programs as well as on the civilian education system. A recent article in *Armed Forces Journal* noted that many senior executives and leaders in both the public and private sectors are "ill-equipped to deal with critical cyberspace issues."[33] Army leaders are responsible for conducting basic tasks, practicing and enforcing cyber hygiene and participating in various cyber activities. Ultimately, Army leaders must have the "ability to interact with the experts and make a decision" when they must "deep dive" on a problem.[34] The development of the generalist portion of the strategy should also review the lessons learned when the Army reinvigorated counterinsurgency doctrine into leader development and education programs between 2005 and 2007.

A centerpiece of the forthcoming Cyber Center of Excellence will be the leader development and education strategy for the cyberspace specialists. Lieutenant Colonel David Raymond's "A Proposed Army Information Dominance Officer Education Model"[35] and Lieutenant Colonel Jason Bender's "The Cyber Planner: Challenges to Education and Understanding of Offensive Cyberspace Operations"[36] are valuable works that offer important observations, insights and recommendations for the Army on cyberspace education. The improvement and maintenance of a dynamic leader development and education strategy for the cyberspace specialists is a substantial task that will provide the fundamental capabilities of the Army's cyber workforce for years to come.

### Personnel

People are the Army's most important investment for achieving cyber security. Despite the rapid growth in the development of cyber professionals, there seems to be an insatiable demand for their employment both within the government and in the private sector. The Army's current cyber workforce construct has various cyber duties and responsibilities dispersed predominately among its signal, intelligence and electronic warfare communities. Retired Army General Keith B. Alexander—former Commanding General, U.S. Cyber Command/Director, National Security Agency/Chief, Central Security Service—has been outspoken about the need for the military services to integrate their information-related capabilities into a single force.[37] ARCYBER and the Army Cyber Institute at the United States Military Academy at West Point, New York, collaborated on the study "Professionalizing the Army's Cyber Career Force" that recommended the creation of an independent cyber branch similar to the Special Forces.[38] On 24 March 2014, the Army established the provisional cyber branch to consolidate officer, warrant officer and enlisted management of the small, highly skilled and highly sought-after cyber population.[39]

Selecting the right cyber professionals is a more challenging endeavor. Cyberspace is so vast and complicated that no one can be an expert on everything. In a recent study, the National Academy of Sciences concluded that "the cybersecurity workforce encompasses a variety of contexts, roles and occupations and is too broad and diverse to be treated as a single occupation or profession" and "because cybersecurity is not solely a technical endeavor, a wide range of backgrounds and skills will be needed in an effective national cybersecurity workforce."[40] The Army has several cyber and cyber-related MOSs and Skill Identifiers but must expand and refine them more frequently to account for the emerging skills and specialties within the rapidly changing cyber profession. This will help the Army's generating force to recruit, access and train the right cyber force.

### Facilities

Facilities play an important role in the Army's success in the cyber domain. Cyber operations centers are an ideal venue to organize and assemble cyberspace experts to meet the security challenges of the cyber domain. The technical capabilities of the facility help define its effectiveness. Operations centers are becoming more prevalent and specialized in both the public and private sectors. In November 2013, Microsoft opened a Cybercrime Center to bring together their security engineers, digital forensics experts and lawyers to help combat fraud, hacking and software piracy.[41] The Army must build and maintain healthy working relationships with other cyber operations centers to improve collective readiness when a crisis demands widespread cooperation and collaboration.

In addition to current operations, the Army must also have institutions that prepare for future cyberspace operations. The Army Cyber Institute at West Point is led by retired Lieutenant General Rhett Hernandez, who served as the first commanding general of U.S. Army Cyber Command prior to his retirement. The institute's mission is to "become a national resource for research, advice and education in the cyber domain, engaging Army, government, academic and industrial cyber communities with the purpose of enabling effective Army cyber defense and cyber operations."[42] The Army Cyber Institute will become the Army's cyber brain trust as it tackles national-level cyber problems and develops a bench of top-tier cyber experts.[43]

### Conclusion

Cyberspace offers both great opportunities and significant challenges. The evolving and expansive nature of the cyber domain has created a complicated and massive virtual environment. The cyber domain has a planetary-level scope with vast interdependencies to the land, air, sea and space domains. The developed world is willing to reap the enormous benefits of cyberspace in spite of its dangers and vulnerabilities. The flow of computer code is near-instantaneous, transcendent of national borders and largely ungoverned. Cyber security is an enormous challenge that has become a national security imperative for the United States.

Cyberspace is ultimately about people. In future wars, strategic landpower—Army, Marines and special operations forces—must have a balance of virtual and physical capabilities to effectively and efficiently impact the will of the people. The U.S. Army has made substantial progress developing capabilities across the DOTMLPF in the cyber domain. There is still work to be done as the Army continues to build the world's most capable cyber force.

- Lead responsibilities for many cyber or cyber-related issues are dispersed among several Army organizations. The Army must capitalize on the creation of the provisional cyber branch and the Cyber Center of Excellence to produce an Army-level unity of effort in the cyber domain.
- Finding the best ways for commanders to integrate cyber capabilities into their formations will improve mission command. The cyber mission forces and the intelligence community have made great strides in this area.
- No one can predict with certainty the next evolution, innovation or breakthrough. The Army must have a robust and balanced investment in modernization and funding for science and technology in cyberspace.
- A small innovation in cyberspace can fundamentally alter the nature of the cyber domain. The Army must remain agile and rapidly evolve its cyber strategy as the cyber domain changes.
- It takes two to three years to educate, train and develop an Army cyberspace specialist. The Army must prioritize recruiting and retention of the most qualified—it cannot afford a perpetual brain drain.
- The cyber domain is at the planetary level and therefore requires a comprehensive effort. The Army must build and maintain healthy working relationships with its unified action partners that include joint, interagency, intergovernmental, multinational, nongovernmental organizational and/or private industry partners. In many cases, the Army may need to share capabilities and help train its partners.

## Endnotes

[1] Chairman of the Joint Chiefs of Staff, "Defending the Nation at Network Speed," delivered at Brookings Institution, 27 June 2013, http://www.brookings.edu/events/2013/06/27-defense-cybersecurity-dempsey.

[2] The global chess analogy was collectively developed during a seminar discussion at the Information Environment Advanced Analysis Course (IEAA) in October 2012. Sponsored by the Office of the Undersecretary of Defense for Intelligence (OUSD(I)), the IEAA equips intelligence, operations and plans personnel with analytic concepts, affiliated techniques and operational constructs that enable graduates to characterize, forecast, target, wargame and assess the information environment to enable commanders to seize and sustain the initiative within the operational environment and reduce risk and uncertainty.

[3] Department of Defense, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010 and amended through 15 December 2013, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[4] "Personally Identifiable Information refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual," accessed on 15 December 2013, http://www.gsa.gov/portal/content/104256.

[5] Miniwatts Marketing Group, "World Internet Users and Population Statistics, June 30, 2012," accessed 21 January 2014, http://www.internetworldstats.com/stats.htm.

[6] Rob Soderbery, "How Many Things are Currently Connected to the 'Internet of Things' (IoT)?" 7 January 2013, accessed 21 January 2014, http://www.forbes.com/sites/quora/2013/01/07/how-many-things-are-currently-connected-to-the-internet-of-things-iot.

[7] Maurice de Kunder, "Daily Estimated Size of the World Wide Web," accessed 21 January 2014, http://www.worldwidewebsize.com.

[8] Dan Kusnetzky, "What is Big Data?" *ZDNet*, 16 February 2010, accessed 27 March 2014, http://www.zdnet.com/blog/virtualization/what-is-big-data/1708.

[9] Gordon Moore, "Cramming More Components onto Integrated Circuits," *Proceedings of the Institute of Electrical and Electronics Engineers*, vol. 86, no. 1, January 1998, accessed 17 January 2014, http://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf.

[10] Nathan Ingraham, "Apple announces 1 million apps in the App Store, more than 1 billion songs played on iTunes radio," 22 October 2013, accessed 21 January 2014, http://www.theverge.com/2013/10/22/4866302/apple-announces-1-million-apps-in-the-app-store.

[11] Allied Business Intelligence Research Mobile Application Research Service, "Android Will Account for 58% of Smartphone App Downloads in 2013, with iOS Commanding a Market Share of 75% in Tablet Apps," 4 March 2013, accessed 21 January 2014, https://www.abiresearch.com/press/android-will-account-for-58-of-smartphone-app-down.

[12] At the Department of Defense, the Joint Requirements Oversight Council (JROC) uses the Joint Capabilities Integration and Development System (JCIDS) as the process to advise the Chairman of the Joint Chiefs of Staff in identifying, assessing, validating and prioritizing joint military capability requirements. JCIDS outputs facilitate changes in doctrine, organization, training, materiel, leader development and education, personnel, facilities and policy (DOTMLPF-P). From Department of Defense, Chairman of the Joint Chiefs of Staff Instruction 3170.01H, "Joint Capabilities Integration and Development System," 10 January 2012, accessed 27 March 2014, http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf.

[13] Department of the Army, Army Regulation (AR) 5-22, *The Army Force Modernization Proponent System*, 6 February 2009 with Rapid Action Revision issued 25 March 2011, pp. 4–5, accessed 6 March 2014, http://armypubs.army.mil/epubs/pdf/r5_22.pdf.

[14] LTC Chevelle Thomas, "Human Resources Command stands up Cyber Branch," *www.army.mil*, 24 March 2014, accessed on 24 March 2014, http://www.army.mil/article/122456/Human_Resources_Command_stands_up_Cyber_Branch.

[15] AR 5-22, *The Army Force Modernization Proponent System*, p. 10, accessed 6 March 2014, http://armypubs.army.mil/epubs/pdf/r5_22.pdf.

[16] A Center of Excellence is a "premier organization that creates the highest standards of achievement in an assigned sphere of expertise by generating synergy through effective and efficient combination and integration of functions, while

reinforcing unique requirements and capabilities," from Department of the Army, AR 5-22, *The Army Force Modernization Proponent System*, p. 10, accessed 6 March 2014, http://armypubs.army.mil/epubs/pdf/r5_22.pdf.

[17] Department of the Army, *www.tradoc.army.mil*, accessed 25 March 2014, http://www.tradoc.army.mil/About.asp.

[18] Department of the Army, TRADOC Regulation 71-20, *Force Development: Concept Development, Capabilities Determination, and Capabilities Integration*, 28 June 2013, p. 70, accessed 6 March 2014, http://www.tradoc.army.mil/tpubs/regs/tr71-20.pdf.

[19] Department of Defense, "Army Announces Decision on Army Cyber Forces," News Release Number: NR-084-13, 19 December 2013, accessed 20 December 2013, http://www.defense.gov/releases/release.aspx?releaseid=16440.

[20] Department of the Army, Field Manual 3-38, *Cyber Electromagnetic Activities (CEMA)*, February 2014, accessed 4 March 2014, http://www.fas.org/irp/doddir/army/fm3-38.pdf.

[21] Department of the Army, "General Order 2014-02," 6 March 2014, affirms the Secretary of the Army's commitment to unity of effort; designates U.S. Army Cyber Command as an Army Force Component Headquarters; reactivates Second Army and designates it as a direct reporting unit; disestablishes U.S. Army Network Enterprise Technology Command/9th Signal Command as a direct reporting unit and reassigns it to Second Army; and designates general court-martial convening authorities with U.S. Army Cyber Command.

[22] Department of the Army, "U.S. Army Cyber Command," accessed 9 April 2014, http://www.arcyber.army.mil/org-arcyber.html.

[23] Department of the Army, "1st Information Operations Command (Land)," accessed 11 March 2014, http://www.1stiocmd.army.mil/Home/Index.

[24] Department of the Army, "311th Signal Command (Theater)," accessed 27 March 2014, http://www.army.mil/311sc.

[25] Department of the Army, "The 780th Military Intelligence Brigade," accessed 11 March 2014, https://www.inscom.army.mil/MSC/780MIB/index.html.

[26] COL Jennifer Buckner, comments during the Institute of Land Warfare contemporary military forum "Building the Army's Cyber Forces . . . Globally Responsive, Regionally Engaged" at the 2013 Association of the United States Army Annual Meeting on 23 October 2013 in Washington, DC.

[27] Siobhan Carlile, "Army recruiting highly qualified Soldiers, DA civilians to serve on new specialized Cyber Protection," *www.army.mil*, 8 October 2013, accessed 21 April 2014, http://www.army.mil/article/112793/Army_recruiting_highly_qualified_Soldiers__DA_civilians_to_serve_on_new_specialized_Cyber_Protection.

[28] LTG Edward C. Cardon, comments during his presentation "Building an Adaptive and Agile Army Cyber Force" at the 2014 Association of the United States Army Winter Symposium on 20 February 2014 in Huntsville, Alabama.

[29] *Ibid.*

[30] For more information on Network Modernization see AUSA's Torchbearer National Security Report "Modernizing LandWarNet: Empowering America's Army" at http://www.ausa.org/publications/torchbearercampaign/tnsr/Documents/TB_Network_web.pdf.

[31] For more information on Network Integrated Evaluations see AUSA's Torchbearer National Security Report "U.S. Army Operational Testing and Evaluation: Laying the Foundation for the Army of 2020" at http://www.ausa.org/publications/torchbearercampaign/tnsr/Documents/TB_ATEC_web.pdf and AUSA's Torchbearer Issue Paper "Capability Set Production and Fielding: Enhancing the U.S. Army's Combat Effectiveness" at http://www.ausa.org/publications/torchbearercampaign/torchbearerissuepapers/Documents/TBIP_CS13_web.pdf.

[32] Institute of Electrical and Electronics Engineers, "Top Technology Trends for 2014," accessed 22 January 2014, http://www.computer.org/portal/web/membership/Top-10-Tech-Trends-in-2014.

[33] Brett Williams, "Cyberspace: What Is It, Where Is It and Who Cares?" *Armed Forces Journal*, 13 March 2014, accessed 19 March 2014, http://www.armedforcesjournal.com/cyberspace-what-is-it-where-is-it-and-who-cares.

[34] *Ibid.*

[35] LTC David R. Raymond, "A Proposed Army Information Dominance Officer Education Model," *United States Military Academy Department of Electrical Engineering & Computer Science Report 1337.1*, 30 September 2013, accessed 17 January 2014, http://www.westpoint.edu/acc/SiteCollectionDocuments/full_paidoem.pdf.

[36] LTC Jason M. Bender, "The Operations Cyber Planner: Challenges to Education and Understanding of Offensive Cyberspace Operations," *Small Wars Journal*, 5 November 2013, accessed 24 March 2014, http://smallwarsjournal.com/jrnl/art/the-cyberspace-operations-planner.

[37] General Keith B. Alexander, "The Army's Way Ahead in Cyberspace," *ARMY*, August 2013, accessed 10 October 2013, http://www.ausa.org/publications/armymagazine/archive/2013/08/Documents/Alexander_August2013.pdf.

[38] Todd Arnold, Rob Harrison and Gregory Conti, "Professionalizing the Army's Cyber Career Force," *United States Military Academy Department of Electrical Engineering & Computer Science Report 1337.2*, 23 November 2013, accessed 17 January 2014, http://www.westpoint.edu/acc/SiteCollectionDocuments/full_pacof.pdf.

[39] Thomas, "Human Resources Command stands up Cyber Branch."

[40] National Research Council of the National Academy of Sciences, "Professionalizing the Nation's Cybersecurity Workforce," accessed 18 September 2013, http://www.nap.edu/openbook.php?record_id=18446&page=1.

[41] Joseph Menn, "Microsoft's new Cybercrime Center combines tactics against hacking groups," Reuters, 14 November 2013, accessed 15 November 2013, http://www.nbcnews.com/technology/microsofts-new-cybercrime-center-combines-tactics-against-hacking-groups-2D11591439.

[42] United States Military Academy, "Army Cyber Institute," accessed 9 April 2014, http://www.usma.edu/acc/SitePages/Home.aspx.

[43] Joe Gould, "Cyber Warfare Research Institute to Open at West Point," *armytimes.com*, 7 April 2014, accessed 8 April 2014, http://www.armytimes.com/article/20140407/NEWS04/304070052/Cyber-warfare-research-institute-open-West-Point.

***Lieutenant Colonel Frank L. Turner II is currently serving as an Army Fellow with AUSA's Institute of Land Warfare.***

ASSOCIATION OF THE UNITED STATES ARMY

**Association of the United States Army**
2425 Wilson Boulevard, Arlington, Virginia 22201-3385
703-841-4300 www.ausa.org