Landpower Essay

No. 14-1
March 2014

An Institute of Land Warfare Publication

Cyberspace as a Weapon System

by

Christopher R. Quick

Introduction

It is undeniable that all who operate in cyberspace must face the reality that every connection of a device to the Internet places networks and users at risk. Once viewed as a commons meant to share information and research across vast distances with ease, cyberspace is now a warfighting domain where longtime enablers (e.g., networks, computer systems, radios) also serve as weapons platforms capable of being used by any and all with the capability and intent. Numerous actors seeking to gain advantage over the United States through its asymmetric exposure to the cyber domain are already maneuvering in that environment and employing the Internet as a weapons platform to achieve their own ends. The threats come from across the global commons as a combinations of automated systems programmed to look for exposed edges in networks and known vulnerabilities in systems, to criminal entities who wish to further their financial gains and independent cohorts of like-minded individuals united to achieve a common effect, to state-sponsored actors who pose a threat based on their own goals.

Cyberspace has become weaponized and the U.S. Army must be prepared to operate, defend and maneuver in that environment.[1] The evidence is easily seen in the reports of attacks by China and its massive industrial espionage efforts,[2] the Stuxnet attack on industrial control systems in Iran,[3] the Shamoon virus in Saudi Arabia[4] and reported attacks on U.S. banks[5] and multiple news agencies.[6] In light of the numerous attacks and exploitations on all types of networks and services with exposure to the Internet, and the pervasive nature of cyberspace, the Army's land domain systems can be used (like any other domain) to conduct operations for nefarious purposes when compromised by any of the numerous actors in the cyber domain. Due to the sheer number of current and projected weapon systems that can potentially operate in this domain, the Army must change the way it views the network from a set of provided services to a weapon system and warfighting platform used in the new global maneuver space known as the cyberspace domain.

The Department of Defense (DoD) generally considers a weapon system to be a "combination of one or more weapons with all related equipment, materials, services, personnel and means of delivery and deployment (if applicable) required for self-sufficiency."[7] However, the dynamic environment and threats in cyberspace demand that this new weapon system be viewed as different from any other system in existence today or in times past. Currently viewed as a communication service, the Defense Information Infrastructure (more specifically the Army's LandWarNet) must be viewed by today's Army not only as a weapons platform capable of connecting Soldiers, sensors and multiple nodes to one another in real time but also as a system

capable of delivering operational effects across the full spectrum of combat operations. As a weapons platform using a variety of capability sets, the network has the potential to disrupt, degrade or deny logical, physical and virtual infrastructure, as well as to damage the components that comprise the effective responsibilities of the modern developed nation state: governance, defense, economic management, provision of health and human services and the maintenance of the infrastructure on which society interacts.

General Keith Alexander, commander of U.S. Cyber Command and the National Security Agency, has stated that cyberspace "is characterized by high levels of convergence of separate and different networks and technology that have come together to form something greater than the sum of the parts."[8] In other words, cyberspace is inherently complex, and operating in this domain demands an integrated approach. Changing the mindset from cyberspace as a facilitator of delivery of a service to cyberspace as an operational warfighting domain allows the Army to shift focus from the customer (e.g., ensuring delivery of e-mail) to mitigation of risks posed by current or potential adversaries and their ability to impact the network. As with many other weapons platforms in the Army, the Assistant Secretary of the Army for Acquisitions, Logistics and Technology—ASA(ALT)—should develop and field this weapons platform and provide appropriate oversight. However, the previous mindset of using cyberspace to deliver services led to a practice wherein numerous organizations developed and fielded different aspects of the service (i.e., enterprise versus tactical), which was not always integrated and synchronized across the force. To shift to a new mindset of employing cyberspace as a weapons system, the consolidation of current systems into a system of systems called cyberspace, managed by a new Program Executive Office (PEO) Cyber, would empower the secretariat to build on established working relationships with Army, DoD and industry cyber partners. This would further ensure that the Army is postured to support the force with an adequately developed, fielded and sustained weapon system with unprecedented speed and accuracy. There are numerous challenges to work through to make this paradigm shift, but these challenges must be overcome if the Army is to gain and maintain its warfighting and technological edge in cyberspace.

Coupled with the new weapon system/platform, the Army must change the paradigm of how this platform is used and employed writ large. Continued technological innovation offers increased opportunities but must include commensurate training and education. The Army's failure to embrace this new paradigm to dominate in cyber as it does on land would aid all those with malicious intent by providing more targets and tools for attack. Therefore, commanders and Soldiers alike must understand and appreciate how to coordinate, synchronize and integrate cyberspace with other warfighting functions. This can be accomplished only through strong leadership, development and training that permeates all of the military communities.

The network as a weapon system

So why change? As directed by the *2010 National Security Strategy* (*NSS*), the United States must now be prepared for asymmetric threats, such as those that target our reliance on space and cyberspace. *NSS* further directs DoD to organize, train and equip for the challenges and opportunities of cyberspace.[9] *The Department of Defense Strategy for Operating in Cyberspace* further amplifies that DoD will treat cyberspace as an operational domain like air, land, sea and space.[10] The Army stood up an operational-level cyber component command to meet these mandates but has yet to fully resource and empower the command with the ability to develop, deploy and employ the weapon systems required to conduct operations as they would in the other domains.

Like the other domains of warfare, cyber units must have weapons platforms to maneuver and engage adversaries within the domain of cyberspace in support of joint and unified land operations. Currently a mixture of fielded equipment, commodity items and services provide a starting point; however, Soldiers and units who conduct cyberspace operations must be equipped and trained with cyberspace capabilities suitable for an operational domain rather than simply relying on enterprise services. This mindset also dictates another change in perspective to treat its operators and those technological solutions as the actual capability. Without a trained operator, a technical solution is useless; without a technical solution, the Army's trained operator

is less effective. Success is dependent upon this mutual relationship, which necessitates their (operator and technical solution) categorization as a capability system in and of itself.

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines a weapon system as a "combination of one or more weapons with all related equipment, materials, services, personnel and means of delivery and deployment (if applicable) required for self-sufficiency."[11] With this definition the case can be made that when cyber warriors fire "bullets" (i.e., scripts, code) from the systems (computers, laptops), Army units are using a cyber-weapons platform to conduct cyberspace operations (disrupt a command and control system) in the information environment.

As a communication service, the Department of Defense Information Network (DoDIN) (and more specifically the Army's LandWarNet) connects Soldiers, sensors and multiple nodes to one another in real time, faster, farther and more efficiently than ever. The ongoing move to a Joint Information Environment (JIE) improves upon the network-based system and moves from multiple separate networks to a single, secure, standards-based joint network. However, the focus remains on shared information technology (IT) infrastructure "with a common set of enterprise services"[12] rather than on a defensible warfighting platform capable of self-sufficiency.

The transformative impact of cyberspace on military operations demands a cohesively developed and managed weapon system that encompasses not only the "single, secure, standard-based joint network"[13] but also a comprehensive array of offensive and defensive cyber capabilities to go with it. These capabilities must complement a network weapons platform that is "the most innovative, efficient, and secure information and IT service in support of the missions, anywhere, anytime, on any authorized device."[14] This change in perspective has the potential to make cyberspace one of the most powerful weapons platforms in the military inventory, as well as to provide a wide variety of political and military ends with serious national security ramifications.

As with other weapons platform/systems, centralized management, governance and oversight are required to rapidly validate and insert developing technologies. As highlighted in the *2013 Weapon Systems Handbook*, "we cannot succeed unless requirements are matched with stable and well-planned resources under sound program management."[15] To guarantee that emerging and critical cyberspace resources receive inclusive and equitable consideration for program-associated funding, requirements for the "network weapons platform" must be integrated and synchronized across the service. This integration, falling under the purview of ASA (ALT), will facilitate a greater mission-focused development and fielding effort. Centralized management sets the conditions for the Army to rapidly design, develop, test and deploy new technologies enabling it to keep pace with the speed of cyberspace operations.

The constant ebb and flow from U.S. Cyber Command's DoDIN Operations, Defensive Cyber Operations (DCO) and Offensive Cyber Operations (OCO) on military networks demands that operational commanders understand the impact of a cyberspace weapons platform on traditional military operations. Balancing the perceived likelihood that aggressors will pay severely for their actions with the ability to provide access to information and functions unabated in the event of an intrusion or disruption will be paramount for a land- and cyber-based Army. This amplifies the need for the Army to fundamentally enhance its capabilities at every echelon and provide a "professional team of elite, trusted, precise, disciplined cyber warriors who defend our networks, provide dominant effects in and through cyberspace, enable mission command and ensure a decisive global advantage."[16]

What must the Operational Army do to change?

Army Strategic Planning Guidance 2013 states that the Army of the future must have a strategy that "empowers and enables Soldiers and squads with improved lethality, protection, mobility and situational awareness."[17] The constant fluid movement—from operating to defending to conducting offensive cyberspace operations—demands that operational commanders understand the impact of cyberspace on traditional military operations. The strategic shift to regionally aligned, mission-tailored forces capable of "ensuring

freedom of maneuver in cyberspace and protecting Army information and the Network"[18] only underpins the need to change the paradigm to network as weapons platform and more specifically how this platform is employed by the Army writ large.

This means making changes to Army formations and to the institutions that develop leaders and Soldiers. Changes must come in both the operational and institutional realms of the Army for this new operating paradigm to take hold. The speed of cyberspace requires new training, skills and understanding by Soldiers charged to employ this new weapon system/platform. Nonstop technological innovation only increases the opportunities for commanders in cyberspace; however, the failure to embrace this new paradigm to dominate in the convergent land and cyber domains will provide more targets and tools for adversaries to attack. The Army must embrace the requirement to provide the knowledge necessary to plan and integrate, as well as to operate, in the cyberspace domain.

Lieutenant General Rhett Hernandez, former commander of Army Cyber Command/Second Army, has stated, "For a command built around technology, it's critical to understand that people are our most valuable asset."[19] For the Army to codify this statement, strong leadership development, training and education programs must permeate its training communities to standardize cyberspace training across unified land operations. Commanders and Soldiers alike must understand and appreciate how to coordinate, synchronize and integrate cyberspace with the other warfighting functions within the information environment. Building a strong knowledge base through institutional education across the officer, enlisted and civilian workforce fortifies the ability of the Army to build combat-ready forces that can be tailored to support land and cyber operations. This drives a multipronged approach to solving the cyber training challenges.

To address the immediate need in cyberspace, a talent management process must be developed to leverage the current inventory of Soldiers and civilians with marked aptitude and problem-solving skills. Pulling talent from across the Army to bring in the best and brightest to tackle to complex problems of cyberspace will enable a stopgap for today, build a baseline cyber force and enable the development of cyber solutions across Doctrine, Organization, Training, Materiel, Logistics, Personnel and Facilities (DOTMLPF) for the cyber forces of tomorrow. This will enable the Army to focus existing personnel with cyber-related attributes on tasks derived from DoDIN Operations, DCO and OCO. This process must be centrally managed and must track those pulled to jump-start the development of the Army cyberspace force. The development of mid-level and senior-level leadership will propagate the hard-fought lessons learned and develop the skills of incoming personnel who arrive with limited or no experience in the application of cyberspace operations.

Next, the development of the future cyberspace force must include the active recruiting, development and retention of skilled, professional Soldiers (active and reserve components), civilians and contractors who can meet dynamic challenges and dominate the cyberspace terrain. Recruitment should be adjusted to measure aptitude and potential for solving complex problems with cyber skills. Cyberspace education must start at initial entry and be promulgated by operational commands and an Army culture that understands the importance of operating in cyberspace on a daily basis. This means nurturing emerging operational and institutional requirements, having them permeate DOTMLPF solutions and integrating them into training and exercises at all levels. The Army should expand and integrate existing operational cyber capabilities of the Army National Guard and Army Reserve to serve as an immediate surge capability to support emerging Army cyber forces.

Finally, there is only one operational environment. To achieve the required know-how to operate in and through the cyberspace domain that is both complex and dynamic, Army leaders must take responsibility for training cyberspace activities at the individual, collective and organizational levels. The sheer number of threats and vulnerabilities, the distributed/dispersed state of current Army networks, a lack of security training and a traditional lack of leadership involvement in cyber security implementations have exacerbated the challenge to transform the Army. The Army can mitigate these risks by implementing leader-directed and leader-managed changes across all levels of Army commands.

The simplest of these changes is for commanders to enforce the bedrock of the Army (standards and discipline) to correct deficiencies and enforce user behavior when operating in cyberspace. The enforcement of cyberspace security and compliance must be likened to any other weapon used during operations. Because cyberspace is transforming how information is created with new forms of content (images, sounds, information and data in multiple forms) and the connectivity used to exchange that content, commanders must take responsibility for both the physical and the virtual environments of the units they command. Cultivating an environment where the standard is to adhere to cybersecurity measures, protection of information and safeguarding of the transportation of information in and through cyberspace will improve the overall combat effectiveness of Army units.

Commanders from the tactical level to the strategic level must not only leverage the capabilities of the cyber combined-arms team with traditional capabilities but must also train them to fight as a cohesive unit to drive favorable outcomes. Demanding access from home station to virtual ranges will significantly impact cyber skills through a combination of live, virtual, constructive and gaming environments for individuals and teams. This essential learning domain will enhance the combined-arms team training in adaptable environments that develop and enhance individual and unit skills while benefiting the overall force during training events. Additionally, many of these training events can be delivered in an economical fashion as a result of efficiencies possible only in the cyber domain.

To truly test the level of training, units and commanders must be challenged with real-world scenarios and force-on-force engagements to hone their ability to conduct decisive-action operations. Facing the Army's world-class cyber opposing force in a myriad of training exercises will provide hands-on experience operating in a contested and degraded environment while enhancing Soldier and leader readiness. This high-reward/low-risk environment further allows Army units to deconflict, synchronize and systematically integrate new methods and mechanisms to seize, retain and exploit the initiative on land and in cyberspace.

Recommendations

Over the past few years, high-profile attacks and exploitation of network systems have highlighted the need for the Army to view its network assets as a weapon system if it is to operate successfully in the cyberspace domain. This weapon system will have the capability not only to connect Soldiers, sensors and multiple nodes in real time but also to deliver operational effects in the complex information environment. Changing the mindset from network as a service to network as a weapons platform allows the Army to shift focus from the customer (e.g., ensuring delivery of e-mail) to adversaries and their ability to impact the network.

Operational units require a network that connects all assets, even in the most austere environments, to deliver decisive results in the shortest possible time.[20] As a weapons platform the network employs a variety of capability sets with the potential to have operational effects across the spectrum of conflict. However, to develop integrated capabilities, coordination and cooperation toward common cyberspace objectives is vital in the acquisition and fielding of new technologies across both the operational and tactical networks. Only unity of effort will allow the Army to keep pace with the speed of operations in cyberspace and adapt to the pervasively transient conditions that await in the future operating environment. Under the oversight of ASA (ALT), the ability to pursue and rethink the technological fundamentals of cyberspace will guarantee that critical cyberspace resources receive equitable consideration for program-associated funding. This further ensures that the Army is postured to support the force with an adequately developed, fielded and sustained weapon system with unprecedented speed and accuracy.

As with any new weapon system/platform the Army must include the corresponding training and education. Failure to embrace this new paradigm to dominate in land and cyber will hinder efforts by commanders at all levels to leverage the cyber combined-arms team with traditional capabilities. Today's environment demands understanding and appreciation of how to coordinate, synchronize and integrate cyberspace training through access to virtual ranges, with adaptable environments, that ultimately impact the cyber skills required in the information environment.

The Army's longstanding dominance on land remains unmatched in the post-Gulf War era. Potential adversaries understand this and are moving rapidly to counter U.S. dominance by leveling the playing field in cyberspace. Maintaining Army dominance in future land warfare requires digitally savvy warfighters, capable of and comfortable with operating in the complex information environment of tomorrow. The Army must adjust the training and capabilities afforded to the force in order to seize the possibilities provided by ever-evolving information technology. Only through a concerted effort to modernize the system of systems that comprises the cyber domain can the Army continue to deliver the advantage required to prevent, shape and win in the land, cyber and human domains.

Lieutenant Colonel Christopher R. Quick is currently the Information Operations branch chief and director of communications synchronization for the U.S. Army Cyber Command/Second Army at Fort Belvoir, VA.

Endnotes

[1] T.P., "Hello, Unit 61398," *The Economist*, 19 February 2013, http://www.economist.com/blogs/analects/2013/02/chinese-cyber-attacks.

[2] *Ibid*.

[3] Jim Finkle, "Researchers say Stuxnet was deployed against Iran in 2007," *Reuters*, 26 February 2013, http://www.reuters.com/article/2013/02/26/us-cyberwar-stuxnet-idUSBRE91P0PP20130226.

[4] Reuters, "Aramco Says Cyber-attack was Aimed at Production," *The New York Times*, 9 December 2012, http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=1&.

[5] NBC News and wire services, "3 more major U.S. banks report possible cyber attacks," *NBC News (Technology)*, 26 September 2012, http://www.nbcnews.com/technology/3-more-major-us-banks-report-possible-cyber-attacks-6126050.

[6] David Garfield, "Stop the Press: Media Outlets Falling Victim to Cyber Attacks," *Huffington Post*, 7 March 2013, http://www.huffingtonpost.com/david-garfield/cyber-security-media_b_2829008.html.

[7] Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 8 November 2010, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.

[8] "Cybersecurity: Preparing for and Responding to the Enduring Threat," Statement of General Keith B. Alexander, USA, Commander, U.S. Cyber Command/Director, National Security Agency/Chief, Central Security Service, before the Senate Committee on Appropriations, 12 June 2013, p. 3, http://www.defense.gov/home/features/2013/0713_cyberdomain/docs/Alexander,_General_Keith_Testimony_6.12.13_Cybersecurity_Hearing.pdf.

[9] President of the United States, *National Security Strategy 2010*, http://nssarchive.us/?page_id=8.

[10] *The Department of Defense Strategy for Operating in Cyberspace*, July 2011, p. 5, http://www.defense.gov/news/d20110714cyber.pdf.

[11] JP 1-02, *Department of Defense Dictionary*, http://www.dtic.mil/doctrine/dod_dictionary/?zoom_query=weapon+system.

[12] Chairman, Joint Chiefs of Staff, "Joint Information Environment White Paper, 22 January 2013, http://www.dtic.mil/doctrine/concepts/white_papers/cjcs_wp_infoenviroment.pdf.

[13] Teresa M. Takai, Chief Information Officer, Department of Defense, Memorandum, subject: Department of Defense Cloud Computing Strategy, http://dodcio.defense.gov/Portals/0/Documents/DOD%20Cloud%20Computing%20Strategy%20Final%20with%20Memo%20-%20July%205%202012.pdf.

[14] *Ibid*.

[15] Assistant Secretary of the Army for Acquisition, Logistics and Technology, *2013 Weapon Systems Handbook*, p. 3, http://www.fas.org/man/dod-101/sys/land/wsh2013/wsh2013.pdf.

[16] Statement by Lieutenant General Rhett Hernandez, Commanding General, U.S. Army Cyber Command/Second Army, before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities Concerning Digital Warrior: Improving Military Capabilities in the Cyber Domain, 25 July 2012, http://armedservices.house.gov/index.cfm/files/serve?File_id=210E8C59-142F-400A-AD8E-9582207686BC, p. 10.

[17] General Raymond T. Odierno, Chief of Staff, Army, and the Honorable John M. McHugh, Secretary of the Army, *Army Strategic Planning Guidance 2013*, http://usarmy.vo.llnwd.net/e2/rv5_downloads/info/references/army_strategic_planning_guidance.pdf.

[18] Statement for the Record by the Honorable John M. McHugh, Secretary of the Army, and General Raymond T. Odierno, Chief of Staff, Army, Before the Committee on Armed Services, United States Senate, First Session, 113th Congress, on the Posture of the United States Army, 23 April 2013, http://www.armed-services.senate.gov/imo/media/doc/McHugh-Odierno_04-23-13.pdf.

[19] LTG Rhett Hernandez, "U.S. Army Cyber Command: Cyberspace for America's Force of Decisive Action," *ARMY*, October 2012, http://www.editiondigital.net/article/Commanding_General,_U.S._Army_Cyber_Command/1197175/128725/article.html.

[20] Odierno and McHugh, *Army Strategic Planning Guidance 2013*, p. 18, http://usarmy.vo.llnwd.net/e2/rv5_downloads/info/references/army_strategic_planning_guidance.pdf.

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