Engaging two domain warfare

LTC Christopher R. Quick

The Army is now a two domain force--LandCyber and warfighters must embrace the contested domain known as cyberspace.

Since the Secretary of Defense announced the creation of a cyberspace-focused command in 2009, a high demand has been placed on each of the Armed Services to provide cyber resources to support to the Geographic Combatant Commands.

The creation of Army Cyber Command represents as a milestone for the Army on its path to operate as a two domain force in Land and Cyberspace. This event, however, was just an initial step towards solving the larger issues of operationalizing cyberspace, changing the culture, developing a work force, and institutionalizing the Army as a two domain force.

One of the factors driving the transformation is an ever growing and increasingly sophisticated threat. With the diffusion of destructive technology, potential adversaries now pose a greater catastrophic threat to our safety than ever. Relying on low cost stand-off technologies to mitigate our Nation's military might, and coupled with the anonymity provided by the internet, today's complex threats will continue to challenge U.S. interests if we do not embrace the newest domain of conflict.

No longer can we look at our military purely as Soldiers, computers and machines leveraged separately to impose our national will during a physical battle. Soldiers and military vehicles equipped with radios, Global Positioning Systems), smartphones, or other electronic devices must now be considered in the virtual sense as well as the physical.

The use of embedded processors in military equipment carried, driven or flown compels senior leaders to think in a two dimensional, LandCyber sense vice a single physical land domain. In all aspects of operational planning, military leaders will have to engage in physical and virtual (cyberspace) planning before an operation. This will allow our forces to operate unabated in cyberspace.

The second factor driving transformation is the increased importance of network-enabled components in military hardware, which has resulted in a virtual military that few could have envisioned. Technology has always enhanced our ability to prevent, shape, and, when necessary, fight and win our Nation's wars. But with the creation of the virtual Soldier, unit, and their associated equipment, the paradigm has changed and so should the military. The ability to conduct military operations through cyberspace means we must be prepared for sophisticated influence operations that leverage cyberspace as a force multiplier and prevent our adversaries from gaining parity. We must, in turn, be prepared to conduct complex cyberspace operations integrated with military operations by integrating capability into force structure.

The U.S. Army must promote increased capabilities within our cyberspace units by populating them with a new generation of digital natives that understands the impact, both real and virtual, digital devices have in today's operating environment. When integrated with digital immigrants - the seasoned veterans who are experienced operating and defending the military's networks through intelligence, computer network operations, information operations, network operations and information assurance - the new generation of digital natives will represent a new breed of Army warrior comfortable with the contested information domain and conversant in cyberspace capabilities.

The Threat

The military's increased reliance on computers and networked devices provides both an opportunity and vulnerability. With the continual expansion of technology and low cost of entry, the operational environment of the future will allow a myriad of threat actors to develop, seize, and exploit advancements in technology. To keep pace with adversaries who rapidly create new and sophisticated ways to capture and exploit data and information. We must understand the risk that comes with the rapid development of capabilities and be prepared to mitigate or accept the risk posed by them.

Today Army warfighters must address the need to operate both on the land and in cyberspace.

Threats in the operational environment (primarily cyberspace) are no longer limited to traditional nation state actors. Instead, they cover potential adversaries that range from rogue individuals to organized groups (like Anonymous and criminal organizations) to sophisticated nation states. The level of sophistication and capabilities presented by this array of adversaries cover a wide spectrum as well. From script kiddies with a laptop or Smartphone engaging in webpage defacement, to attacks like Titan Rain and Moonlight Maze in which U.S. government computers were targeted by organized hackers with access to immense computing power. Collectively, these potential adversaries converge to create a dynamic environment operating outside traditional geographic boundaries and allegiances.

Cyberspace threats also pose a different type of risk than past threats. The span of control in cyberspace creates continuous friction among networks as a range of actors with various affiliations, cultural backgrounds, and strategic goals wrestle to control the global domain of cyberspace. The ability to distribute cyberspace assets (both physical and virtual) increases the threat within cyberspace as physical elements (machines and users) cross into the virtual realm using one of many distributed access points, leverage operational information, and then create realworld (physical) consequences in the other operational domains. This cross domain ability requires commanders to control not only physical access but also virtual access to the critical information and systems used to achieve operational objectives.

Perhaps the most challenging aspect of the threats posed in cyberspace is the difficulty in attributing actions to the responsible actor with any level of certainty or confidence.

Introducing attacks through microwave, thumb drives, portable media, and satellite communications, individuals or teams carrying out attacks can do so remotely, from the safe confines of a neutral, unaware country, while masking their true location and identity through proxies (both man and machine).

While the ability to forensically assess which actor, organization, or nation was behind an attack has improved, the problem remains that the Internet enables anonymity (through virtual personas) that deters security.

Evidence of the changing threat dynamic and the potential for devastating effects can be seen in three examples. The first is an early form of LandCyber in the conflict between Russia and Georgia in August 2008. Georgia's national communication infrastructure, to include government websites, news outlets, and banks, were the focus of a distributed denial of service attack.

People supporting the Russian cause attacked (virtually) immediately prior to Russian military forces entered Georgia's borders for ground operations (Land).

The second example is the attack on InfraGards (a web security partner organization with the FBI) website in February of this year by the Anonymous hacker group. The group stated that "We broke into their web server, perused their assorted presentation materials, and finally deleted everything and vandalized their website."

The last example, which has garnered the world's attention, is the computer attack on Iran's Natanz uranium enrichment plant. The attack resulted from a worm (called Stuxnet) which used four zero-day exploits to disrupt the rotational frequency of the enrichment plant's centrifuges. According to an International Atomic Energy Agency report, this attack severely damaged Iran's nuclear program.

These three attacks highlight several key aspects of cyberspace operations. One, that offensive cyberspace capabilities can cause physical damage; two, such effects can be used independently or in

(Continued on page 28)

In the 21st Century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communication networks and assured access to cyberspace.

- DoD 2010 Quadrennial Defense Review Report

(Continued from page 27)

concert with traditional military operations; and three, that cyberspace presents an opportunity and vulnerability for our Nation's military.

Why a Change is Required

Without a doubt technology has forced a paradigm shift by altering how we view today's operational environment and that of tomorrow.

The ubiquitous presence of digital technology at the tactical level has created a digital presence for each tactical unit, soldier and vehicle that was not thought of before. Just as we seize, retain and exploit the initiative to gain a position of relative advantage in the land domain, we must also do the same in cyberspace.

The increasing array of technology available to individual Soldiers, from biometrics to global positioning systems to Smart phones and tablet computers, means that wherever the soldier is in the world, cyberspace follows, as do its inherent risks.

The use of embedded processors in military equipment - whether carried, driven, or flown - compels military leaders to think in a two dimensional (LandCyber) sense vice just a physical domain (Land) sense.

In all aspects of operational planning, military leaders must now consider both the physical and virtual (cyberspace) domains when planning an operation. The transition from Soldiers with a tactical radio and map to LandCyber soldiers with multiple electronic and digital devices represents the evolution of two dimensional Soldiers whose virtual persona must be factored along with their physical presence. Commanders must understand their units' digital persona as well as the physical, and that their command can be virtually tracked, located, attacked, and destroyed just like the physical unit can.

Voice and data networks that once operated separately have converged and now enable the delivery of multiple forms of media – text, audio, and video – over the same wired, wireless, or fiber-optic infrastructures of the Internet. The benefit of this converged Army network is that it functions as a central nervous system for every unit, connecting leaders to their forces. The ability to communicate, see the battlefield, and maintain situational awareness depends on access to the Army's networks. Not only must the commander account for his digital persona, he must also ensure confidence in the integrity of the network while engaged in the contest of wills. Thus, the cyberspace contest is not an ethereal struggle, but an integral element of a units' ability to shoot, move, and communicate.

While technology improves conditions for the ground commander to achieve the stated objectives, connecting to today's networks also connects the commander and the unit to other friendly, neutral, and adversarial audiences and actors.

This means cyberspace enables commanders to better visualize, describe, direct, lead, and assess the operational environment by giving them greater access to reliable information. In short, LandCyber enables mission command by helping commanders and their staffs better assess the character and impact of the information environment in their operational area. To fully benefit from this improved information awareness, commanders and their staffs must understand cyberspace as a 'combat arm.'

Lastly, the Army has been directed, (in the Department of Defense Strategy for Operating in Cyberspace) to focus on three areas of potential adversarial activity: theft or exploitation of data; disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources; and destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems. Leaders, however, lack sufficient situational awareness and understanding of cyberspace to manage risks and exploit opportunities. The Army has no common level of Soldier "digital awareness" across its ranks.

Keeping Pace with Technology Changes

The operational environment contains a wide range of clever, adaptive adversaries who can impact the Army's networks with small-scale technologies. They collect intelligence on the U.S. to determine vulnerable IP components and electronic apertures for key systems and highly selective cyberspace, electronic, and kinetic takeouts of key nodes. They can influence our national will and decision cycle through social media, internet chat rooms, blogs, and international media. Their ability to impact a military operation through cyberspace means we must be prepared for sophisticated influence operations (both kinetic and non-kinetic) that leverage cyberspace as a force multiplier and prevent our adversaries from gaining parity. To be prepared to conduct complex cyberspace operations integrated with military operations, we must integrate capability into force structure.

Technology has always been considered an enhancement to our ability to prevent, shape, and win the wars of the U.S. But as the creation of the virtual soldier/unit and associated equipment has changed, the paradigm, the military must also change. Operations in cyberspace can occur nearly instantaneously. Army forces can attack or be attacked in cyberspace at a rate not achievable in the other domains. Depending on the degree

of interconnectivity, this can happen over vast distances at near the speed of light. The tempo in which these activities take place poses a requirement for speed in decision making heretofore not known or required. Legacy processes, methods, and equipment must yield to new concepts and equipment that compensate for the fluid, dynamic, and contested domain of cyberspace (must be based on people, technology, and applications).

The United States has created, developed, and deployed many innovations in the hardware and software sectors during the information age. Yet other countries now move just as quick in technology sectors and their ability matches or exceeds ours in some arenas. To maintain our advantage in the information environment, the US military must synchronize tools, personnel, protocols, and machines into rationally persuasive systems that can effectively operate at network speed.

An efficient use of a system of systems (man, machine, and applications) will promote finding, fixing, mitigating and resolving threats to our networks and military operations.

Successful operations will require the development of integrated cyberspace intelligence collection capability with cyberspace operations to facilitate mission command and operational effects across the other warfighting domains. With multiple opportunities to inflict damage through malicious activity, the actions of a few individuals has forced a paradigm shift in how commanders view mission command as well as preserve the rapid free flow of information sharing required in today's environment.

ADP 3-0 (dated October 2011) states that "Unified land operations describes how the Army seizes, retains, and exploits the initiative to gain and maintain a position of relative advantage in sustained land operations through simultaneous offensive, defensive, and stability operations in order to prevent or deter conflict, prevail in war, and create the conditions for favorable conflict resolution." The Army, however, lacks sufficient cyberspace capability and capacity, as well as the integrated Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities construct necessary to effectively support commanders accomplishing this task as part of the Army's Prevent/Shape/Win strategy. Developing an integrated LandCyber construct will better inform commanders and staffs how to support not only the Army but Joint requirements as well.

We must devise a "Smart Defense" approach to pool, share, and specialize capabilities as needed to meet 21st century challenges.

Leveraging the Next Generation

While technology plays an important role in the cyberspace, it is not the technology that will win on the 21st century's cyberspace battlefields. Rather, people will make the difference. The U.S. Military must cultivate cyberspace units by populating them with a new generation of digital natives who understand how digital devices influence both the real and virtual environment. These digital natives will use their knowledge of the dynamic rules and culture of cyberspace to enhance the ability of leaders/commanders to achieve their military objectives. The U.S. Army must recruit, develop, and retain skilled, professional Soldiers (active duty and reserve component), and DA civilians in a highly competitive environment.

The development of LandCyber Warriors to gain physical, temporal, and psychological advantages over an enemy will enable us to execute cyberspace operations from people-built cyberspace war fighting platforms. Teams of cyberspace warriors will use these cyberspace platforms to support both Army and Joint requirements. We do not yet, however, have the human capital or authorities to make all this work.

As the demand for cyberspace personnel has increased so has the challenge of retaining personnel with current skill sets.

The Army must create (or modify existing) talent management processes to leverage current Soldiers and civilians with pronounced learning aptitude and problem solving skills. This will allow the Army to focus existing personnel with cyberspace-related attributes on tasks derived from DOD Global Information Grid Operations, Defensive Cyber Operations and Offensive Cyber Operations. However, the overall cost of this endeavor is a greater monetary cost to develop a skilled cadre. As discussed at the March 2012 Land Cyber Summit: Additional skills + additional training + more senior positions = higher dollar cost per individual.

Although our Nation faces serious challenges in access, training, developing, and retaining Soldiers and Civilians to effectively operate in cyberspace, the current work force provides an interim solution. This solution involves the utilization of current Army professionals in the Intel, Signal, EW and IO communities who have desired cyberspace skill sets and expertise. These skill sets include 35Qs, 35Ns, 35Ps, 352Ns, 352Ss, 353Ts, 255Z, 255A, 255N, 255Ss, 25As, FA26s, FA29s, 290As, 29Es, FA30s.

These personnel can provide the initial framework for establishing cyberspace/electro-magnetic Cells at ASCC down to brigade level and for building cyberspace warfighting formations and headquarters.

To address its shortage of trained cyberspace personnel the Army should use the wide range of existing opportunities in the personnel inventory today.

(Continued on page 30)

(Continued from page 29)

These opportunities (bonuses, reclassification, assignment of choice) will require adequate resources and modification (must measure aptitude and potential technical skill) to be properly used in support of enhancing effectiveness. Additionally, by packaging on-going efforts into a comprehensive cyberspace recruiting strategy, the Army can adequately address and remedy its recruit, train, and retain gaps.

Paramount to any cyberspace workforce solution is the inclusion of tailored civilian management process. Current information and tracking systems are insufficient to support detailed understanding, identification, assignment, management and tracking.

There are positive attributes associated with the Civilian workforce excepted and competitive services; however, neither program is sufficient by itself, which requires further analysis.

Last, the cyberspace workforce should have access to training from a variety of venues that offer a common educational platform/portal that provides robust environments to develop and enhance skills of the force. Access to training should include virtual ranges and training environments that simulate challenges that test individuals and team capabilities. This capability should encompass the ability to access operational SME's and leaders that can facilitate training in either institutional or operational environments.

Conclusion

Without doubt the Army is now a two domain force (Land-Cyber). As such, it must embrace cyberspace as an operational domain. Army Cyber Command provides the foundation from which the Army can leverage its ability to operate in Land and Cyberspace. However, since we have transitioned to LandCyber, the Army can no longer look at its forces purely as Soldiers, computers and machines that are leveraged separately to impose our will during battle.

The long list of potential adversaries with the capability to pose catastrophic effects will continue to threaten U.S interests if we do not face and embrace the newest domain of conflict.
The growing number of Soldiers and military vehicles equipped with radios, GPS devices, and other electronic devices demand consideration in the virtual sense as well as the physical.

The two dimensional ideology (LandCyber) must permeate the decision cycle and operational planning of military leaders if we are to prevent, shape, and when necessary, fight and win our Nation's wars. The ability of our adversaries to impact a military operation through cyberspace demands that the Army prepare for sophisticated influence operations that leverage cyberspace and prepare to conduct complex Land-Cyber military operations.

Finally, the U.S. Military must cultivate cyberspace units by populating them with a new breed of digital natives comfortable with digital devices in the future information environment both real and virtual. Combined with seasoned digital and information veterans who have operated and defended the militaries networks the Army will not only successfully operate in cyberspace, but become Second to None in Cyberspace.

LTC Christopher R. Quick *is currently the Director of Strategic Communications for the U.S. Army Cyber Command / Second Army at Fort Belvoir, VA. His assignments include Fire Support Officer, Battery Executive Officer, Brigade Assistant Operations Officer, and Brigade Fire Direction Officer. He commanded a Battery with 1st Battalion, 17th Field Artillery. He served in the 41st Signal Battalion, 1st Signal Brigade as a Battalion Automations Officer. LTC Quick served as Brigade Information Operations Officer with the 2nd Brigade, 101st Airborne, where he served a tour in Iraq. He has served on the Army Staff within the Army G3/5/7 in DAMO-ODI and served on the Army Cyber Task Forces as the lead action officer for the development of Army Cyber Command. LTC Quick holds a B.S. degree from Park University in Kansas City, Mo. and an M.S in Computer Science and another in Information Operations from the Naval Post Graduate School in Monterey, Calif.*

Join the Discussion
https://signallink.army.mil

Acronym QuickScan

C/EM - Cyberspace/Electro-magnetic
DCO - Defensive Cyber Operations **DDoS** - Denial of service attack
DGO - DOD Global Information Grid Operations
DOTMLPF - Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities
FBI - Federal Bureau of Investigation
GCCs - Geographic Combatant Commands
GPS - Global Positioning Systems
OCO - Offensive Cyber Operations
SME - Subject matter Expert