Strategy Research Project

# LandCyber Operations: A Double Edged Sword or a Dream Team?

by

Lieutenant Colonel John L. Rafferty, Jr.
United States Army


United States Army War College
Class of 2013

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*



| **1. REPORT DATE** *(DD-MM-YYYY)* | **2. REPORT TYPE** | **3. DATES COVERED** *(From - To)* |
|---|---|---|
| xx-03-2013 | STRATEGY RESEARCH PROJECT | |

**4. TITLE AND SUBTITLE**
LandCyber Operations: A Double Edged Sword or a Dream Team?

**5a. CONTRACT NUMBER**

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**
Lieutenant Colonel John L. Rafferty, Jr.
United States Army

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
Colonel Charles J. Tulaney
Department of Military Strategy, Planning and Operations

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

**10. SPONSOR/MONITOR'S ACRONYM(S)**

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION / AVAILABILITY STATEMENT**
Distribution A: Approved for Public Release. Distribution is Unlimited.

**13. SUPPLEMENTARY NOTES**
Word Count: 6,145

**14. ABSTRACT**

Recognizing the inseparability of the land and cyberspace domains as well as the requirement to dominate both, the Army has developed the LandCyber operations strategy which goes beyond cross-domain operations and proposes a partnership that seeks to unify the effects created through cyberspace and land dominance. This monograph describes LandCyber in theory and then in action through the lens of the Army's Prevent, Shape, Win operating construct. At first glance, the LandCyber strategy looks like a dream team for commanders, but further examination reveals its threat as a double edged sword. Will LandCyber enable micro-managing leaders to be the "wet blanket" of mission command? Or will it open new doors for more effective maneuver and influence operations? The Army should embrace the LandCyber strategy as an approach for operations in the current and future environment.

**15. SUBJECT TERMS**
Cyberspace, Mission Command, LandWarNet

| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON** |
|---|---|---|---|---|---|
| **a. REPORT** | **b. ABSTRACT** | **c. THIS PAGE** | | | **19b. TELEPHONE NUMBER** *(Include area code)* |
| UU | UU | UU | UU | 34 | |

USAWC STRATEGY RESEARCH PROJECT

# LandCyber Operations: A Double Edged Sword or a Dream Team?

by

Lieutenant Colonel John L. Rafferty, Jr.
United States Army

Colonel Charles J. Tulaney
Department of Military Strategy, Planning and Operations
Project Adviser



U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

## Abstract

| | |
|---|---|
| Title: | LandCyber Operations: A Double Edged Sword or a Dream Team? |
| Report Date: | March 2013 |
| Page Count: | 34 |
| Word Count: | 6,145 |
| Key Terms: | Cyberspace, Mission Command, LandWarNet |
| Classification: | Unclassified |

Recognizing the inseparability of the land and cyberspace domains as well as the requirement to dominate both, the Army has developed the LandCyber operations strategy which goes beyond cross-domain operations and proposes a partnership that seeks to unify the effects created through cyberspace and land dominance. This monograph describes LandCyber in theory and then in action through the lens of the Army's Prevent, Shape, Win operating construct. At first glance, the LandCyber strategy looks like a dream team for commanders, but further examination reveals its threat as a double edged sword. Will LandCyber enable micro-managing leaders to be the "wet blanket" of mission command? Or will it open new doors for more effective maneuver and influence operations? The Army should embrace the LandCyber strategy as an approach for operations in the current and future environment.

**LandCyber Operations: A Double Edged Sword or a Dream Team?**

> Perhaps it is best to see the Internet and cyber attack as the latest in a long line of technologies that have changed warfare and provided new military capabilities.
>
> —James Andrew Lewis[1]

The US Army Cyber Command's strategy for LandCyber operations provides a window from which one might peer into the future and see a network centric force that has harnessed technology and information to achieve advantage in the land and cyberspace domains by establishing unity of command. While on one hand, the LandCyber strategy is a good start in terms of conceptualizing how the Army will operate in an increasingly networked manner, on the other hand, one might be concerned that the Army's reliance on a network will make it more vulnerable to an attack through cyberspace. Protecting the network, however, will be a core competency of future cyber forces and demonstrates commitment to mitigating that risk. As Army units operate at the end of a long tether in an increasingly complex and distributed land and cyber environment, the Army's network will provide opportunities for incredible access to information gathered from both the land and cyber domains which will then be shared vertically and horizontally. This is where both opportunity and vulnerability lie. Will the Army use LandCyber delivered enhanced situational awareness and access to information to improve its capability to Prevent, Shape and Win the nation's wars, or will it allow technology to be the wet blanket of mission command? Will LandCyber be a double-edged sword that is ultimately self defeating, or a dream team of complementary capabilities? The land and cyberspace domains are inseparable and the Army must embrace the LandCyber strategy as an approach for operating in the current and future operating environment.

The Department of Defense (DoD) 2011 Strategy for Operating in Cyberspace states that "cyberspace is a defining feature of modern life" in which billions of people "connect, socialize, and organize themselves."[2] Ever increasing access to and reliance upon information delivered through cyberspace has elevated cyberspace's recognition to that of a domain of military operations. The 2010 DOD Quadrennial Defense Review justified the designation by stating that cyberspace is "now as relevant a domain for DoD activities as the naturally occurring domains of land, sea, air and space." The US Army's LandCyber White Paper 2013-2020 takes it a step further in describing the cyberspace domain as "terrain" for the information environment.[3] Even a cursory study of the relative short history of cyberspace, specifically the internet, very clearly illustrates its vulnerability to attack, hacking, criminal activity, espionage and cyber war. Cyberspace is a truly contested domain. But in spite of the obvious risk, reliance on cyberspace for information continues to grow for both the US Army and the world. The US Army must be able to protect itself and exploit advantages in the cyberspace domain.

Land, perhaps a more tangible and familiar domain of military operations, is also a contested domain. US interests will continue to be threatened across the globe. Competition for natural resources, clashes of culture and religion, grasps for political power, economic tension and overpopulation are but a few of the underlying conditions that will foment conflict in the 21st century. History has not proven an effective road map for determining the location of the next conflict but it has shown its likelihood. America's Army must remain ready to win decisively and dominate the land domain.

If thoroughly grasped by commanders, LandCyber has great potential for units to achieve effects in the cyberspace domain that will contribute directly to decisive effects in the land domain. The unified effects will enable commanders to attacks less tangible centers of gravity, such as political will, through the cyberspace domain. Cross domain effects will complement and support each other to achieve far more decisive effects in the operational environment.

The 2012 Army Posture Statement addresses the land and cyber domains by proposing even closer cooperation as a requirement for the future. "As demonstrated in the last decade, the information environment has changed the way we fight. Military and cyberspace operations have converged...This requires the Army to be dominant in both the land and cyberspace domains."[4] Building on this idea, the 2d US Army/Army Cyber Command (ARCYBER) has developed a concept for LandCyber unified operations. This concept goes beyond cross-domain operations and proposes a partnership that seeks to unify the effects created through cyberspace and land dominance. This partnership relies on the successful employment of LandWarNet, the Army's portion of the global information grid (GIG), and will be enabled through the mission command warfighting function. The Commanding General of ARCYBER, LTG Rhett A. Hernandez, describes this concept as an "opportunity for the Army to dominate in LandCyber. We're focused on integrating at all levels in order to ensure mission command in the conduct of unified operations. This all about maintaining our freedom to operate while taking it away from the enemy."[5] The Army should embrace the LandCyber strategy as an approach for operations in the current and future environment.

## Israeli Defense Force Example

When examining the Israeli Defense Forces (IDF) execution of Operation Pillar of Defense against Hamas in Gaza during the second half of 2012, one can see a future in which land and cyberspace operations become more closely aligned in order to achieve cross domain synergy. The IDF has a well established cyber enabled precision guided weapon capability to destroy adversary infrastructure and kill adversary leadership. When compared to dramatic kinetic success against Egyptian forces in previous wars, IDF efforts to kill and destroy irregular force targets were not as decisive in Lebanon, Gaza, or the West Bank. While achieving some military success, Israel was largely condemned in the international community and the Palestinian and Lebanese populations. In September 2006, the IDF conducted a very sophisticated offensive cyber attack to disrupt state-of-the-art Syrian air defenses followed by a successful precision guided bomb attack that destroyed a nuclear facility.[6] While effective in eliminating a perceived threat, Israel failed to exploit their success in the information environment. On the contrary, they never admitted to it nor justified their actions. As expected, during Operation Pillar of Defense the IDF conducted offensive cyber operations to disrupt enemy command and control and precision guided attacks and intelligence driven maneuver operations to kill enemy combatants –all impressive applications of cyber power to enable kinetic operations. What was not expected was the IDF's use of cyber power in the battle for ideas. The IDF conducted an aggressive social media campaign to compete in the information environment through messages that provided accurate, real-time conflict justification, warnings, successes, and situation reports to a wide variety of audiences, friend and foe alike.[7] Even if the long term

effects of these new efforts are not yet known, the point is well taken – the cyberspace domain is about more than computer network attack and precision guided munitions, it lends itself to domination of the information environment.

## LandCyber

The Army's LandCyber White Paper states that "LandCyber is a strategy to apply unified force (Land and Cyber) under a single mission commander to establish optimal combination of effects to influence the threat before it can impact friendly forces and operations."[8] To some, the introduction of cyber capabilities may seem revolutionary but no more than an airplane dropping bombs in World War I or Army amphibious operations in World War II or even Counterinsurgency operations in Iraq. As in the case of the previous examples, LandCyber is an evolution of the combined arms concept and the Army is well suited to integrate cyber capabilities into existing formations to achieve even greater effects. ARCYBER forces exercise five operational functions in cyberspace domain: Build the network; Operate the network; Defend the network; Exploit networks; Attack networks. [9] Most Army units are able to construct tactical networks and operate them effectively but as the networks grow in size and complexity so does their vulnerability and thus each BCT will require a more sophisticated ability to build, operate and defend the network than currently exists with assigned signal personnel and current equipment.

Army Cyberspace Operations are comprised of three distinct missions: Defense Information Network Operations (DINO), Defensive Cyberspace Operations (DCO), and Offensive Cyberspace Operations (OCO). DINO refers to the functions required to build, access and sustain the Army cyberspace network. Eventually, this network will

be the LandWarNet which will be discussed later in this paper. DCO refers to the "passive and active operations to preserve the ability to utilize friendly cyberspace capabilities and protect networks and net-centric capabilities."[10] OCO refers to the set of functions that enable Army commanders to achieve effects in the cyberspace and land domains. [11]

ARCYBER developed Cyberspace Mission Areas as a framework for operationalizing the cyberspace missions.[12] A description of these mission areas will help understand the advantages they offer to Unified Land Operations (ULO). These mission areas are Cyberspace Mission Control Area, Cyberspace Force Enhancement Mission Area, Cyberspace Support Mission Area, and Cyberspace Force Application Area.[13] The mission control area includes necessary actions to operate and defend the network. These include passive and active measures, such as cyber network hunting and incident response. The force enhancement area includes the functions that provide for situational awareness and knowledge while the support mission area refers to the operations that support the LandWarNet. The force application mission area includes exploit, attack and influence operations. Understanding the Army's cyberspace potential in operational terms is essential to grasping the LandCyber strategy.

While LandCyber is dependent on the Army's future network (LandWarNet), the LandCyber strategy must be broad enough to convince commanders that considering the cyberspace domain and taking advantage of cyber capabilities is not just about more computers and "cyber attack." With the possible exception of the Army's most specialized formations, computer network attack (CNA) and computer network exploitation (CNE) are competencies which are not currently resident in Army general

purpose forces and focusing on those two capabilities will only serve to frustrate and mislead commanders. In fact, the authorities for these operations are complicated and contain interagency legal issues that are out of bounds for Army units who do not possess the skill sets or equipment. ARCBYER is developing a process and capability that would serve as a "call for fire," of sorts, to request effects by, with, or through the cyberspace domain.[14] The Army must provide clarity to the LandCyber strategy by presenting it as a concept that will deliver and maintain situational awareness, to an extent not previously experienced, which will enable decisive maneuver and effective information operations to assist commanders in achieving their mission.

## LandWarNet

Army units at every level need reliable access to information technology that helps sift through the data to gain knowledge through the cyberspace environment, enabling decisive maneuver and an ability to conduct influence operations, in a more efficient and timely manner. LandCyber operations enabled by LandWarNet and brought to life through the mission command warfighting function will provide unprecedented access to information and the technology and staff functions that will lead to gaining knowledge.

The Army Posture Statement for 2012 states "The Army network must be dynamic to give Soldiers, civilian and partners information and services when and where needed." The embodiment of that vision will be LandWarNet. LandWarNet is the US Army's effort to create the "enterprise-level network that will enable warfighters and leaders around the world to achieve information superiority." There are 5 major goals for the program. First the program seeks to operationalize LandWarNet through efforts to

enable warfighters at the tactical level. The Joint Tactical Radio System (JTRS) and the Warfighter Information Network-Tactical (WIN-T) are examples of on-going efforts to get secure voice, data and video "on the move" capabilities into the operational force.[15] Second, LandWarNet must improve the Army's cybersecurity position. Moving information and computing functions to the "cloud" will dramatically reduce the network's vulnerability.[16] The third objective is to improve operational effectiveness while gaining efficiencies across the network. The Network Integration Evaluation (NIE) is a proactive collaboration with industry to ensure technological development is compatible with the network BEFORE it becomes available "on the shelf." [17] Fourth, LandWarNet must enable joint and partner collaboration and will do this through clear standardization efforts for the Common Information Environment and everything over internet protocol (EoIP) network procedures. And finally, the LandWarNet community must attract and retain talented Soldiers and civilians. [18] It is a long term equipment modernization and force structure program designed to deliver a significantly enhanced capability for the Army of 2020 while still improving the Army's existing information network along the way.

In fact, the Army will begin to field 8 LandWarNet integrated capability sets to brigades beginning in 2013.[19] These sets will introduce emerging network technology improvements to the operational force "in stride." Tactical and operational use by mainstream units will provide feedback to the LandWarNet community for continued improvements. Through unit testing and the NIE, the Army will be able to refine the network architecture to create an "end to end" solution for warfighters with a data strategy for Army wide common products and services. Mobile devices made "user

friendly” by Apps 4 the Army (A4A) will ensure the network is available to users in need – the warfighter at the tactical edge.[20]

LandWarNet contributes directly to the LandCyber concept through the mission command warfighting function. LandWarNet’s overarching purpose is to “deliver a deployable network enabled mission command capability” as the “cornerstone of the Army’s expeditionary force capability.”[21] This is absolutely critical to the LandCyber concept which relies entirely upon increased access to the network. As the warfighting function responsible for integration, the mission command warfighting function will provide the framework for integrating Cyber capability in support of ULO.

Mission Command - the warfighting function

Army Warfighting Functions (WfF) are "groups of tasks and systems (people, organizations, information, and processes) united by common purpose that commanders use to accomplish missions. [22] The Army WfFs are movement and maneuver, intelligence, fires, sustainment, protection and mission command. Under the LandCyber concept, ULO requires action in both the land and cyberspace domains which happens to span all seven WfFs. According to ADRP 6-0,"the mission command warfighting function integrates the other warfighting functions into a coherent whole....it provides purpose and direction to the other warfighting functions."[23] The ARCYBER concept for LandCyber operations seeks to utilize the Mission Command Warfighting Function (WfF) to bring the land and cyberspace domains together and gain synergy from complementary cross domain activities to achieve decisive effects on land.

The Mission Command Center of Excellence (MCCoE) is the Army’s center for developing and integrating mission command Doctrine, Organization, Training,

Manning, Leader Development, Programs and Facility requirements and solutions across the six warfighting functions. Of the MCCoE's ten priorities, three are clearly pointed at LandWarNet and Cyber efforts which demonstrate the close nature of the LandWarNet, cyberspace, and mission command relationship. The MCCoE is involved in the Agile Process/NIE for materiel solutions, the Improve Mission Command Initiative to create better command post and information technology, as well as partnering with Army Cyber to "ensure mission command."[24] Mission command serves as both a WfF for balancing the art of command with the science of control as well as a guiding principle for "how to lead." In terms of "leading", mission command is the "conduct of military operations through decentralized execution based upon mission-type orders."[25] These mission type orders are based on trust and shared understanding of the situation which is where the technology aspect comes into play. Shared understanding comes from information technology delivered friendly force tracking devices, common pictures of the environment, enemy and terrain, as well as communication systems that enable routine reporting. The MCCoE must ensure that the LandWarNet solutions for the mission command WfF serve the master of the mission command principle of leadership.

The LandCyber strategy should be a guiding principle for commanders, similar to combined arms, and mission command. The Army doesn't "do combined arms" but we operate in a combined arms fashion. The Army does not "do mission command" yet seeks to operate in a mission command fashion. The Army will never "do LandCyber" operations yet LandCyber will enable combined arms, mission command and create opportunities for the Army to compete in the battle for ideas.

## Influencing People

The Army Cyberspace Force Application framework outlines three capabilities that deliver effects to commanders on the battlefield - Exploit, Attack, and Influence. [26] Exploit and attack are too complex for near term serious application in traditional Army formations. Cyberspace influence operations offers commanders the greatest opportunity for increased near term capabilities. Unleashing the potential of influence and influence activities (IIA) through cyberspace may finally provide commanders the opportunity to properly match actions and message and to compete effectively in the battle for ideas. These ideas form the basis for desired human behavior. Whether that behavior is hostile to United States interests or merely supportive of hostile actors, the US Army must compete for those ideas. The world is more connected than ever and increasingly its people get their information from cyber sources – internet sites and social media. Hostile actors may require kinetic activity to change their behavior but most people's behavior can be altered through the use of information.

One could argue that information is the central theme in current and future conflict. Using the Clausewitzian trinity model that features an influencing idea (policy) at the top, chance (military competitors), and emotion (the people) as the legs of the triangle, it becomes clear that information is central to the very concept of conflict. If one were to truly use Clausewitz' position with regard to a center of gravity then one would not target an adversary's strength but rather the focal point where that strength is distributed, where that strength gains power.[27] Building on that position, if an idea is the unifying theme that supports conflict then information might be defined as the idea's strength and so the focal point, the point of distribution, might be the internet or

cyberspace. To place this in the context of the Global War on Terrorism, which undeniably is a contest of ideas - religious extremism centered on hatred of the west is the motivating idea. Information from various antagonistic sources can provide the idea's strength but the means by which the information is distributed and the place where it gathers strength, the focal point, often lies in the infinite reaches of cyberspace. Contrary to popular sentiment, this center of gravity for ideas is not necessarily the place where one strikes for victory but rather it is the place where one must compete, and if centers of gravity exist at multiple levels of war then LandCyber offers commanders at all levels new capabilities to identify capabilities and exploit vulnerabilities.

Globalization's tsunami effect on the information environment shows very clearly the requirement for the Army to compete in the cyberspace domain.[28] In order to do so, the Army needs to execute IIA with speed, agility, mass and resilience. Speed of information flow requires the Army to engage in a continuous fashion - proactively, reactively and as a matter of course. Agility requires the Army to react quickly to changes in the environment, operational adjustments, friendly or enemy action - agility made possible through enhanced situational awareness. Mass refers to the requirement to “carpet bomb” the information environment. In this context, precision refers to information engagements done in person while resilience is the requirement for Army networks - well defended from attack and robust enough for huge servings of information. When high volume, timely and responsive information operations to inform and influence target audiences are coupled with kinetic and non-kinetic operations that match the information objectives, commanders will have created the opportunity to

affect the unifying idea and ultimately change behavior. Since information is central to the motivating idea and thus central to conflict, the Army must adopt the LandCyber strategy as a way to more effectively compete for the ideas of people.

Over the course of operations in Iraq and Afghanistan, information operations have been hindered by restrictions that prevented BCT level units from conducting effective and timely information operations. In most cases, these restrictions were based on historical information fratricide or a fear of information fratricide based on routinely lousy situational awareness. In some cases, it has been a lack of trust that subordinate units would make the correct decisions with regard to information operations based on current conditions they had encountered. It is counter intuitive that the Army tends to trust more when the stakes are high with respect to loss of human life or mission accomplishment in extreme conditions.

"Little Groups of Paratroopers" (LGOPs) is an example of that trust or risk acceptance. Once Paratroopers exit an aircraft they are on their own to link up in small groups before they make contact with their parent units. LGOPs then operate without direct supervision basing their actions solely on their understanding of the operation and their commitment to accomplishing the commander’s intent. The Army tends to entrust Soldiers and leaders with where to drop a bomb, who to shoot in a firefight, or when to turn in a tank because leaders are familiar with the environment which enables them to understand and measure the risk. Some Army leaders cannot extend trust when operating in unfamiliar territory because human nature influences leaders to unnecessarily control or restrict what they don't really understand. Cyberspace and the information environment is an example of that unfamiliar terrain. Cyberspace

operations will make that environment more familiar to all personnel while technology enabled mission command will enhance situational awareness for commanders. Perhaps then will commanders extend their trust into IIA.

## Current Situation

The mainstreaming of Cyberspace operations into unified operations has already started. The Army recently moved to formalize cyber-electromagnetic activities (CEMA) into doctrine.[29] However, this move potentially boxes cyber activities into a dark corner of a Tactical Operations Center if a less enlightened commander refuses to acknowledge the potential of LandCyber strategy. There are three distinct lines of operation for CEMA: cyberspace operations, electronic warfare (EW), and electromagnetic support operations (EMSO). Cyberspace operations employ capabilities to create effects in or through cyberspace through the employment of offensive cyber, defensive cyber or global information grid operations.[30] EW controls or denies the electromagnetic spectrum through electronic attack and electronic protection whereas EMSO coordinates electromagnetic spectrum operations and prevents frequency fratricide.[31] While this definition is potentially confusing given the EW and EMSO additions, it recognizes their unique relationship and captures the basic operational functions defined by ARCYBER and gets cyber "into the fight." Much as the development of the network is a long term project, so is the integration of CEMA into staff processes and operations. ARCYBER and the MCCoE are "co-leads in the Army's effort to determine how best to accomplish CEMA integration for the long term."[32] In the interim, units will create CEM working groups in order to bring together the WfFs and the integrating cells (Plans, Operations, Future Operations).

## LandCyber in Context

The 2012 Army Posture Statement states that the role of the Army is to prevent, shape and win the nation's wars. Just as no war has been won without boots on the ground, no future conflict will be exclusive of the cyberspace domain. [33] The next portion of this monograph explores examples of LandCyber operations in the prevent, shape, and win construct.

## Prevent

Preventing future conflict involves demonstrating credible military options that serve to dissuade a potential adversary - regardless of the domain or domains in question. Prevention actions with respect to LandCyber operations include manning and training the force, preparing for future conflict as well as defending the Army's network from attack. Army formations will continue to cycle through the Army's Force Generation (ARFORGEN) process during which they will be manned, equipped, and trained to high levels of readiness. As discussed earlier, Army BCTs will begin to receive portions of the LandWarNet program in the next year as well as stand up CEM cells. The new 35Q military occupational specialty, cryptologic network specialist, is being aggressively recruited by the Army.[34] As LandWarNet matures and gets fielded incrementally to Army units, cryptologic specialists will fill the ranks of units to help deliver enhanced capabilities to commanders. Additionally, the 780th Military Intelligence Brigade has been activated as "the BCT of cyber" with the mission of defending military networks and potentially addressing the “cyber call for fire” requirement.[35] Many units will complete their training cycles with challenging rotations at one of the Army's three training centers. The training centers will feature a "World

Class Cyber Opposing Force" from the 1st Information Operations Command to create a realistic multi domain training environment.[36] This initiative will challenge units, generally BCTs, as they create and defend networks. If able to defend their network, these BCTs will enable mission command, achieve shared situational understanding and compete in the informational environment. Through the NIE/Agile Process, the Army will deliver materiel solutions that will enhance command post capability with respect to communications, analysis, and situational awareness. A powerful example of anticipated capabilities involves common social network analysis and social media analysis programs on common hardware working off "the cloud" where the "network is the computer."[37] Through the cyber domain, land force CEM, intelligence, targeting, and operations personnel will be manned, equipped, and trained to understand human behavior of particular groups. The full complement of LandCyber possibilities will be tested against an adversary in the land and cyberspace domains. Between the purpose built 780th MI Brigade and the enhanced BCTs, the Army will demonstrate a remarkable capability - a force that is ready for deployment and prepared to dominate in the land and cyberspace domains.

## Shape

Shaping the international environment involves activities to "assure our friends and contain our enemies."[38] The regionally aligned force concept is designed to provide a wide range of Army capabilities to Combatant Commanders in support of theater security objectives.[39] The Army Deputy Chief of Staff G3/5/7 described the concept as being "all about providing the Combatant Commander with the right force at the right time to better shape the region, maybe preventing something like an Iraq or

Afghanistan."[40] Though regions, partners and objectives vary considerably, one can easily speculate that theater security objectives might include building partner capacity in cyberspace practices and cyberspace defense. BCTs and other units operating in Africa, for example, may be forced to build, operate and defend their own networks in order to operate successfully from distributed locations. Partner nations who are able to operate alongside the Army in the land and cyber domains may prove to be more capable partners in the future. The Commanding General of US Army Africa envisions regionally aligned Army units operating in distributed locations across the continent who may not necessarily intervene in local conflicts but who would help train and equip local forces and assist host nation governments.[41] Building partners, with traditional security related capabilities, who can defend their networks and information systems, will create partners who are interoperable on our networks. More reliable partners on a trusted, effective network will result in increased situational understanding for all parties - both deployed and at home station preparing for future operations. The regional immersion will give CEMA operators and opportunity for a network and information environment reconnaissance aided by local partner guides. CEM, intelligence and targeting personnel from a regionally aligned force deployed will gain an understanding of the information environment, perhaps aided by a local cyber guide, and access to information for social media and social network analysis. Using open source information units will be able to determine valuable information through the use of mainstream analysis programs that contain algorithms which determine relationships between people and organizations based on a wide variety of variables- communications, location, contact, finances, etc.[42] The information sharing

opportunities for units working through the ARFORGEN cycle will result in regionally aligned forces that will actually be "regionally aware." Using the ARFORGEN and regionally aligned force concept, as one unit is regionally deployed, another unit will be preparing to deploy, even as another is resetting from deployment. LandWarNet will connect all units to the network regardless of their place in the ARFORGEN cycle and offers incredible opportunities for real time collaboration and learning. Using a simple knowledge model - Oblivious, Ambiguous, Inquisitive, Facilitative- one can easily understand the advantage a future force will possess.[43] A deploying force with little to no understanding of the environment would be categorized, using this construct, as Oblivious. After a period of immersion the unit would reach the level of Ambiguous - aware but uncertain. Eventually, the unit would reach levels of Inquisitive, asking the right questions, and later attain the level of Facilitative, doing the right things. With the additional information access enabled by LandWarNet, the possibility exists for units to attain the level of Inquisitive before deployment. Another powerful shaping capability delivered by deployed regionally aligned force will be their IIA actions which will demonstrate to the local and international community the strength of local forces, the mutually shared interests and values, as well as the matched up messages and actions. Through this combination of activities in the land and cyberspace domains the Army will be able shape the security environment - better partners, informed audiences, more prepared forces, more connected and stronger networks, better intelligence and overall higher levels of readiness.

## Win

Using a forcible entry and introduction of a follow on force scenario, one will be able to see the value of the LandCyber concept during decisive operations – the win portion of the construct. The Army maintains an airborne BCT as part of the Global Response Force for the large scale airborne assault and airfield seizure portion of the joint forcible entry mission. Based on the IDF cyber attack against Syrian air defenses, one could imagine how offensive cyber at the strategic level could enable a forcible entry mission to penetrate hostile airspace. Currently airborne forces have very little situational awareness en route to the drop zone short of that which they gained during the mission analysis and rehearsal process. While current mission command systems such as Command Post of the Future (CPOF), intelligence systems and E-mail are integral to large Tactical Operations Center provided power and networks, airborne forces are almost completely reliant upon analog mission command systems. With maps and line of sight radios, the airborne force works through traditional battle tracking. After the airfield is seized and the runways cleared, the initial aircraft land with vehicles which brings limited digital mission command systems and then requires battalions and the BCT to go through the process of converting from analog to digital mission command - laboriously entering data into Blue Force Tracker devices, laptop computers and other devices in an effort to establish situational awareness horizontally across the BCT and then vertically up to the joint task force commander.[44] Once the airfield is ready to receive airplanes to deliver the decisive force, speed is essential. The airfield can become a target rich environment full of taxiing airplanes and slow moving vehicles. The optimal course of action would be for combat units to link up and

move straight from the airfield to follow on positions – immediately employing decisive combat power. Unfortunately, a digital hand-off means does not currently exist. Units do not have a way to share situational awareness which slows down the transition and the expansion of the lodgment – increasing risk.[45] The LandCyber strategy offers the potential to change this archaic process. Using the previous example of shaping operations, imagine the situational awareness that the entire joint task force would have based on shared information from a regionally aligned force's experience. Beginning an operation with information like a social media network diagram or a social network diagram would give the forcible entry and decisive forces a decided advantage - they would start from a position of advantage in the learning model because they will understand the information environment as well as the terrain. The entire joint task force would have a common understanding of how to conduct traditional and IIA operations to change the behavior of the adversary without alienating the local populace. With a real-time common operational picture of the land and cyberspace domains and a real plan for IIA operations, lower level units will be able to operate in a permissive information environment based on the local conditions they encounter.[46] Current conflict has demonstrated reluctance to allow initiative inspired IIA operations at lower levels because of the threat of information fratricide.[47] The CEM cells will be able to advise the commander on actions to take in the cyber electromagnetic spectrum with respect to protecting his network and shutting down the adversary's information access. The Defense Advanced Research Projects Agency has been testing tablet computers with transformative smart phone applications in Afghanistan which are delivering mapping, networking and individual identification capabilities at the platoon

level conducting combat operations.[48] Mainstream delivery of this type of device as part of the LandWarNet A4A program will significantly increase the situational awareness of the airborne assault force while providing the same level of information to the follow on force - simultaneously. Approaching LandCyber strategy and embracing cyber capabilities organized to deliver effects by, with and through the cyberspace domain, in a combined arms manner, will clearly make the Army more effective along the prevent, shape, win mission construct.

## Concerns

While the scenarios provided in the previous section illustrate the possibilities offered by LandCyber, the Army cannot afford to fall victim to the attractive siren of technology and ignore the possible risks. Cyber enabled information in the form of a common operational picture, network diagram, or on-line profile, regardless of their level of detail, have never adequately described reality and usually beg for more information.[49] Situations will exist in which platoon leaders, brigade commanders and division commanders will have the same common operational picture yet different ideas of what actions should be taken. In the future as in the present, some commanders will practice mission command by empowering and enabling subordinates with intent while others will micro-manage subordinate commanders with specific instructions and over-bearing supervision. But in a network enabled force, micro-managing commanders will be able to cast a wider net and potentially paralyze an entire organization. If LandCyber cuts twice as a double edged sword, it will surely strike a fatal blow to mission command.

However, if LandCyber is a dream team, the future of mission command has never been brighter. Commanders are not the only cause of mission command failure; often it is the inexperienced subordinate who lacks the intuitive ability to see opportunities even in the best of mission command circumstances. With common situational awareness and reliable voice and data communications, a more experienced commander can act as a coach in the ear of a platoon leader to guide him in the right direction while remaining within the spirit of mission command. With the recent emergence of “machine learning” that offers applications for analyzing human behavior and decision making, language translation and pattern recognition, it is not much of a stretch to imagine a platoon leader with a “learning machine” on his forearm which can make recommendations for action based on months of input data and shared situational awareness.[50] That kind of capability would surely meet the goal of LandCyber - “to ensure mission command in the conduct of unified land operations.” The right kind of leader with the right kind of technology - that is a dream team.

## Conclusion

"A century ago, armies discovered that technology could be the key to victory. Since then there has been a steady stream of new weapons, new technologies, and new ways to attack."[51] This monograph proposed that unified land and cyberspace operations as an operating concept is the next step in the evolution of combined arms and the continued effort to harness technology. The Army's operating concept of Prevent, Shape, and Win is well supported by the LandCyber operations approach at all levels in order to achieve strategic effects. A more full examination of cyber operating functions through each element of the Prevent, Shape, Win construct will help

commanders to understand how the “LandCyber approach” will enable them to orchestrate complementary effects in both domains. LandCyber implementation should parallel LandWarNet. Each deliverable from the LandWarNet program that improves the Army’s network capability ought to be accompanied by an incremental increase in commander effectiveness in achieving cross domain synergy. Further development of the cyber attack “calls for fire” to higher level cyber units will allow the Army to realize that potential when it becomes available. Given the emphasis by the Army's most senior leaders on mission command, almost to the point of promising that type of leadership environment to junior leaders, the Army cannot allow LandCyber to renege on that promise. Further study must examine the impact of LandCyber operations on mission command. As for the Army’s LandCyber strategy, it’s a good place to start.

## Endnotes

[1]James Andrew Lewis, "Cyber Attacks, Real or Imagined, and Cyber War," Center for Strategic and International Studies, July 11, 2011, http://csis.org/publication/cyber-attacks-real-or-imagined-and-cyber-war, (accessed January 11, 2012).

[2]U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace*, (Washington, DC: U.S. Department of Defense, July 2011), 1.

[3]U.S. Department of the Army, Army LandCyber White Paper 2013-2030 (pre-decisional draft), (Washington DC: US Department of the Army, December 20, 2012),10.

[4]John M. McHugh and Raymond T. Odierno, The Nation's Force of Decisive Action: 2012 US Army Posture Statement to the 112th Congress, 2nd Session, (Washington DC: U.S. Department of the Army, 2012), 3.

[5]LTG Rhett Hernandez, "Tactical and Operations Cyberspace Modernization: The CEM Element," Briefing Slides, Baltimore, MD, AFCEA Land Forces East Meeting, August 16, 2012, 2.

[6]Sally Adee, "The Hunt for the Kill Switch," *IEEE Spectrum,* May 2008, 12.

[7]Brian Fung, "Inside Israel's Social-Media Command Center," *The Atlantic Monthly,* November 25, 2012, 14.

[8]U.S. Department of the Army, Army LandCyber White Paper 2013-2030,18.

[9]LTG Rhett Hernandez, "Tactical and Operations Cyberspace Modernization", 9.

[10]U.S. Department of the Army, Army LandCyber White Paper 2013-2030, 23.

[11]Ibid., 24.

[12]Ibid.

[13]Ibid.

[14]Joe Gould, "ARCYBER goes on attack, on paper and in training," *The Army Times,* December 17, 2012.

[15]Association of the United States Army, *Modernizing LandWarNet: Empowering America's Army*, Torchbearer National Security Report, (Arlington, VA: Institute of Land Warfare, May 2012), 3.

[16]Ibid., 4.

[17]Ibid.

[18]Ibid., 3.

[19]LTG Susan G. Lawrence, U.S. Army Chief Information Officer, "Appendix 2 to Annex M (LandWarNet) to the U.S. Army Campaign Plan 2012," Washington, DC., M-2-3.

[20]LTG Susan G. Lawrence, U.S. Army Chief Information Officer, "Appendix 1 to Annex M (LandWarNet) to the U.S. Army Campaign Plan 2012," Washington, DC., M-1-1.

[21]LTG Susan G. Lawrence, U.S. Army Chief Information Officer, "Appendix 2 to Annex M (LandWarNet) to the U.S. Army Campaign Plan 2012," Washington, DC., M-2-1.

[22]U.S. Department of the Army, *Unified Land Operations*, Army Doctrinal Reference Publication 3-0, (Washington, DC: U.S. Department of the Army, May 16, 2012), 3-2.

[23]U.S. Department of the Army, *Mission Command*, Army Doctrinal Reference Publication 6-0, (Washington, DC: U.S. Department of the Army, May 17, 2012), 1-4.

[24]Mission Command Center of Excellence Trifold, *Enabling Commanders and Leaders,* (Ft Leavenworth, KS: U.S. Army Combined Arms Center, June 1, 2012).

[25]U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011), 3.

[26]U.S. Department of the Army, Army LandCyber White Paper 2013-2030, 25.

[27]Antulio J. Echevarria II, *Globalization and the Nature of War*, Strategic Studies Institute Monograph, (Carlisle Barracks, PA: US Army War College), 17.

[28]Ibid., 1.

[29]Wayne A. Grigsby, et al, "CEMA: A Key to Success in Unified Land Operations," *ARMY*, June 2012, 43.

[30]Ibid., 44.

[31]Ibid.

[32]Ibid.

[33]John M. McHugh and Raymond T. Odierno, The Nation's Force of Decisive Action, 5.

[34]Joe Gould, "Proactive Cyber Soldiers Make up Brigade, New MOS," *The Army Times,* December 17, 2012.

[35]Ibid.

[36]Joe Gould, "ARCYBER Goes on Attack, on Paper and in Training," *The Army Times,* December 17, 2012.

[37]Enrique J. Reyna and Dennis J. Castellanos, "Exploiting Weakness: An approach to counter cartel strategies," Monograph submitted to the Naval Postgraduate School, (Monterey, CA: U.S. Naval Postgraduate School, December 2011), 77.

[38]John M. McHugh and Raymond T. Odierno, The Nation's Force of Decisive Action, 6.

[39]Association of the United States Army, "Regionally Aligned Forces Offer a New Army Model for Global Involvement," http://www.ausa.org/meetings/2012/annualmeeting/Pages/AMStory_Regional.aspx, October 2012, (accessed January 11, 2013).

[40]David Vergun, Guard, "Reserve to Strengthen Regionally Aligned Brigades," www.army.mil/article/89685/,October 31, 2012, (accessed January 11, 2013).

[41]Association of the United States Army, "Regionally Aligned Forces Offer a New Army Model for Global Involvement."

[42]Enrique J. Reyna and Dennis J. Castellanos, "Exploiting Weakness: An approach to counter cartel strategies,", 82.

[43]William J. Polania, "Leveraging Social Networking Technologies," Monograph submitted to the Naval Postgraduate School, (Monterey, CA: U.S. Naval Postgraduate School, September 2010), 82.

[44]Curtis A. Buzzard, "Map Board to CPOF: An Airborne Infantry Battalion at JRTC and the Challenges to Providing Situational Awareness during an FSO Rotation," *Infantry*, April/May 2011, 12.

[45]Ibid., 13.

[46] Eric V. Larsen, et al., *Understanding Commanders' Information Needs for Influence Operations,* (Santa Monica, CA: Rand Corporation, 2009), 58.

[47]Ibid., 59.

[48]Spencer E. Ante, "Military Takes Apps to War," *Wall Street Journal,* September 4, 2012.

[49]Zadie Smith, "Generation Why," *New York Review of Books*, November 25, 2010.

[50]Rachel Ehrenberg, "Software Scientist: With a little data, Eureqa generates fundamental laws of nature," *Science News*, January 14, 2012, 46.

[51]James Andrew Lewis, "Cyber Attacks, Real or Imagined, and Cyber War," Center for Strategic and International Studies, July 11, 2011, http://csis.org/publication/cyber-attacks-real-or-imagined-and-cyber-war, (accessed January 11, 2012).