Cyberspace Operations in Support of Counterinsurgency Operations

by

David W. Pendall
Ronald Wilkes
Timothy J. Robinson

The Institute of Land Warfare
ASSOCIATION OF THE UNITED STATES ARMY

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
10 APR 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyberspace Operations in Support of Counterinsurgency Operations	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Association of the United States Army,The Institute of Land Warfare,Attn: Director, ILW Programs, 2425 Wilson Boulevard,Arlington,VA,22201**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**20**	

AN INSTITUTE OF LAND WARFARE PAPER

The purpose of the Institute of Land Warfare is to extend the educational work of AUSA by sponsoring scholarly publications, to include books, monographs and essays on key defense issues, as well as workshops and symposia. A work selected for publication as a Land Warfare Paper represents research by the author which, in the opinion of ILW's editorial board, will contribute to a better understanding of a particular defense or national security issue. Publication as an Institute of Land Warfare Paper does not indicate that the Association of the United States Army agrees with everything in the paper but does suggest that the Association believes the paper will stimulate the thinking of AUSA members and others concerned about important defense issues.

LAND WARFARE PAPER NO. 95, April 2013

Cybersecurity Operations in Support of Counterinsurgency Operations

by David W. Pendall, Ronald Wilkes and Timothy J. Robinson

Colonel David W. Pendall is an Army War College Fellow at the Massachusetts Institute of Technology's Lincoln Laboratory Security Studies Program. In his previous assignment he was the Combined Joint Intelligence Officer for Regional Command–East/CJTF-1 in Afghanistan and concurrently the Intelligence Officer of the 1st Cavalry Division. He has served in key leadership positions within U.S. Army Europe, V Corps, Multinational Corps–Iraq, NATO/International Security Assistance Force, National Security Agency/Central Security Service and other tactical-level units. Pendall holds a B.A. from Ohio University, an M.S. from Central Michigan University and a Master's in Military Art and Science in Theater Operations from the Army's School of Advanced Military Studies.

Lieutenant Colonel Ronald Wilkes, U.S. Army, is currently assigned to U.S. Strategic Command. He served previously with the Army Cyber Command, 1st Information Operations Command, 18th Military Police Brigade and the 3d Infantry Division. Wilkes holds a B.S. from Savannah State College, an M.A. from Webster University and an M.S. from George Mason University.

Major Timothy J. Robinson, U.S. Marine Corps, is a Communication and Information Systems Officer stationed with Marine Forces Cyberspace Command. He has held numerous positions with the 9th Communication Battalion and served as an Operations Research Analyst at Marine Corps Logistics Command. Major Robinson holds a B.S. from Virginia Polytechnic and State University and an M.S. from the Naval Postgraduate School.

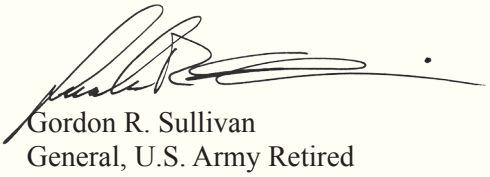
Inquiries regarding this and future Land Warfare Papers should be directed to: AUSA's Institute of Land Warfare, Attn: Director, ILW Programs, 2425 Wilson Boulevard, Arlington VA 22201, e-mail *sdaugherty@ausa.org* or telephone (direct dial) 703-907-2627 or (toll free) 1-800-336-4570, ext. 2627.

Contents

Foreword

This paper provides a perspective on how best to use cyberspace operations in support of U.S. military operations in Afghanistan. The authors describe the nature of cyberspace operations in general, discuss the need for enhanced cyberspace operations and express a viable way ahead for future cyberspace operations in Afghanistan. They posit that additional research and coordination should be conducted to better define and develop requirements for cyberspace capabilities, command and control of cyberspace operations and integration of activities in a manner that supports the International Security Assistance Force commander, the operations of regional commanders and related strategic shaping and global counter terrorism pursuit operations. The lessons we learn now while fighting the counterinsurgency (COIN) fight will serve us in future conflicts.

It has become apparent there is more work to be done in exploiting our adversaries' use of cyberspace. Insurgents and members of their supporting cells have been captured on the battlefield with all imaginable types of digital media and Internet-capable devices. Insurgents and terrorist organizations all have an online presence that is becoming more sophisticated and useful to their operations. Thus, the authors argue that it is both clear and essential that efforts to counter our enemies in the Afghan COIN fight must evolve and become more effective. Our next adversary may be well funded and technologically literate, originate from a more educated society and may have developed a comprehensive cyber operations doctrine. This paper was designed to provoke additional thought about cyberspace operational relevance, suggest necessary change and enable future success in Afghanistan and future conflicts.



Gordon R. Sullivan
General, U.S. Army Retired
President, Association of the United States Army

10 April 2013

Cyberspace Operations in Support of Counterinsurgency Operations

Introduction

The United States has fought an innovative, ruthless and persistent enemy in Afghanistan for more than 11 years. In response to an evolving adversary, the U.S. military developed counterinsurgency (COIN) doctrine to create a framework for commanders to view their operational environment (OE) and provide new methods of applying all the capabilities at their disposal. Comprehensive COIN operations are the basis of International Security Assistance Force (ISAF) campaign planning and tactical operations. While COIN provides a comprehensive strategic framework to use in defeating an insurgency, it lacks any substantive analysis concerning the value of employing cyberspace operations.

America's enemies understand the power of technology. The entry cost to using digital communications is low while the reliability, quality and simplicity of service are generally high. Open-source intelligence indicates that insurgents use different technologies to communicate, create operational plans, store institutional knowledge and develop strategy. The full extent of insurgents' employment of their technological portfolio with respect to command and control, financing, recruiting, training, propaganda dissemination and knowledge management remains an unknown. These issues are of particular concern, as they indicate a level of sophistication that can enable and potentially enhance operations against coalition forces. Present insurgent and/or terrorist cyber-based activities are not fully understood at the operational and tactical levels. The purpose of this paper is to describe the nature of cyberspace operations in general, discuss the need for enhanced cyberspace operations in Afghanistan and express a viable framework for how future cyberspace operations could be more effectively conducted in Afghanistan.

Description of Cyberspace Operations

Cyberspace operations provide support to traditional military operations and, within some rare cases and specific opportunities, replace them. Technological solutions, either offensive or exploitive, assist intelligence and operational planners in targeting individual insurgents or insurgent networks, operating within a larger social network wherein they gain support from the

cyber domain. By understanding the digital patterns of life established by insurgents and supporting organizations, U.S. forces can conceptually develop enemy communication models and better understand their operations and tactical processes. This information improves friendly situational awareness and adds context to existing knowledge bases.

In some cases, cyberspace operations can replace physical military activities by supporting, enabling, informing and influencing activities. Instead of conducting a direct-action raid that can unduly risk maneuver forces, a deceptive cyber operation may be more suitable to shape the target, set favorable conditions for use of kinetic force or disrupt cohesion within the network. Efforts such as these can cause an adversary to commit a desired action that will provide a tactical advantage for U.S. forces. Exemplar cyber operations can cause a number of problems, including but not limited to disrupting target patterns of life, destroying trust among key actors in enemy networks and delaying or disrupting logistics or financing. Cyber operations can provide a substantial military effect if resourced, coordinated and executed properly and synchronized with other kinetic- and non-kinetic-based effects. Furthermore, these actions may provide military planners with reflections across a network, confirming or denying existing estimates about threat operational frameworks and insurgent tactics, techniques and procedures.

Establishing Terms of Art and Science

In 2008, senior military leaders within the Joint Chiefs of Staff defined cyberspace operations and its component parts, settling some of the more contentious discussions within the U.S. cyber community.

Cyberspace operations are defined as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[1] Cyberspace capabilities are comprised of many different elements—such as computer software, networks and other technologies—that interact with digital or analog communications. As described in Joint Publication 3-13, *Information Operations*, cyberspace operations consist of computer network attack (CNA), computer network exploitation (CNE) and computer network defense (CND).[2]

CNA is defined as "actions taken through the use of computer networks to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves."[3] CNE is "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[4] Finally, CND is characterized as involving actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks.[5]

The Need for Agile Cyberspace Operations in the Afghanistan Theater of War

Insurgent organizations and the larger supportive network have several points of presence on the Internet. Wherever there is access to the Internet, there is the probability it is being used for strategic communication, information operations (IO), advertisement for recruits, solicitation of funding and ongoing discussions by insurgent organizations. The proliferation of cellular-based technologies, particularly 3G (the third generation of mobile communication

technology), has expanded insurgents' capability sets.[6] The implication for coalition forces is that insurgents will progressively gain greater access to cellular devices, some Internet capable, likely aiding them in command and control of their forces. Insurgents will continue to leverage these capabilities in opposition to coalition forces, Afghanistan National Security Forces and the Government of the Islamic Republic of Afghanistan (GIROA).

It would be naïve to think insurgents such as the Taliban, the Haqqani Network or other negative influences in Afghanistan lack the ability or interest to use information technology to increase their effectiveness. The threats to a stable Afghanistan are comprised of different factions with different motivations for fighting or maintaining instability. While they may be categorized as primitive, cruel, resourceful and committed to opposing the GIROA and coalition forces, they also possess a superior cultural attunement that the coalition does not. Being poor and uneducated does not equate to being unresourceful, unintelligent or incapable of developing and adopting combat enablers. The events of the Arab Spring in 2011 indicate the power of common technologies in countries with some of the world's lowest Internet penetration levels.[7]

While the current Internet penetration level in Afghanistan can also be considered low, there are indicators that it may not remain so in the near future.[8] The following table shows growth in Afghanistan-based service providers and usage statistics from 2010 to 2011:

Table 1

Telecom Statistics at the end of December 2011[9]

	2010	2011	% Growth
GSM Providers (Licensed)	4	4	0
GSM Subscribers	14,855,235	17,558,265	15%
Internet Service Providers	7	7	0
CDMA Subscribers	96,947	134,092	27%
Landlines	63,533	80,607	21%
Investments in $ Millions	1,563	1,787	12.5%
Telecom Base Stations	3,822	4,428	13.6%
Population Coverage	Over 80%	Over 85%	5%

GSM – Global System for Mobile Communication
CDMA – Code Division Multiple Access

There is a clear and growing consumer base for GSM and Internet services. Over the next three years, Afghanistan's Ministry of Communications and Information Technology (MCIT) plans to spend $215.96 million in support of the National E-Afghanistan Program, which "provides an opportunity to bridge the communications gap that exists within the country whilst also creating new systems of data and information management within a model of new public management."[10] Since MCIT improvements will benefit Afghanistan as a whole, insurgents will also be further enabled by these improvements.

Currently, physical and technical conditions contribute to limits on technology accessibility in Afghanistan. To some degree, these limitations hamper insurgents' exploitation of this communication medium. Barriers to development range from Afghanistan's mountainous geography to poor information technology infrastructure. Lack of technical expertise in the Afghan workforce may limit the ability of insurgents to recruit suitable technicians to support

their operations. As access to technology and the Internet improves, barriers to communication will decrease significantly and perhaps radically. Metcalf's Network Law explains that user networks' value expands geometrically due to the addition of new nodes.[11] Currently, there are a number of private Afghanistan-based efforts to increase overall access to the Internet and communications technologies. Projects are in development to emplace fiber-optic cables to improve connection speeds and reliability. Implementation plans and advertising exist for 3G- and General Packet Radio Service-based networks, which will mark a significant jump in effective penetration of Internet services.[12] Coupled with likely decreases in pricing, the use of Very Small Aperture Terminals will rise in more remote areas of the country. While there are difficulties in accessing Internet technology, there remains a strong desire to develop and use it in daily life, as witnessed by individuals' attempts to access the information domain via broadcast radio, television and personal devices connected to the Internet. As the information environment in Afghanistan becomes more accessible, use by insurgents and their supporting networks will become routine.

Cyberspace Operations in Support of Counterinsurgency and Stability Operations in Afghanistan

An insurgency is defined as "an organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict."[13] In Afghanistan, the insurgency is not a monolithic group of Afghan-based fighters. Numerous armed groups are fighting for different purposes; some are strategic in nature, while others have more materialistic or self-serving objectives. U.S. and coalition forces are wading through this shifting battlefield by creating innovative and effective solutions to complex problems. Counterinsurgency is defined as "military, paramilitary, political, economic, psychological and civic actions taken by a government to defeat insurgency."[14] Integrating cyberspace operations alone will not pacify or defeat the insurgency in Afghanistan but provides a fast-developing opportunity for creating significant effects in the overall COIN fight.

While no single element of national or international power will decisively shift momentum, cyberspace operations' support to COIN will take on increasingly important roles. One such core role is in complementing intelligence operations to capitalize on the existing use of the Internet by insurgents. Intelligence support to countering insurgent use of the Internet begins with defining the OE though the intelligence preparation of the battlespace (IPB).[15] IPB is "the systematic, continuous process of analyzing the threat and environment in a specific geographic area."[16] To conduct effective cyberspace operations, one must understand the characteristics and composition of the social network and the overall cyberspace environment. A cyber IPB (CIPB) is critical to provide planners with the information required to understand and effectively target insurgents in the cyberspace OE. Cyber-based targets have a physical presence. Planners must understand the physical, logical and persona layers affecting their battlespace in order to conduct operations.

Technology and its uses are dynamic; the constant change requires consistent observation and evaluation for cyberspace situational understanding and operations. CIPB efforts must be adjusted to reflect changes to physical and logical structures of the cyberspace environment. Planners, to the greatest extent possible, must be able to forecast expansion, crossover, migration and additions to the digital topology that may affect U.S. cyberspace operations.

One solution to providing full-spectrum cyberspace operational support to COIN is to have a centralized and integrated planning and execution capability in theater to support the

commander in achieving theater-based objectives. Integrated theater cyber operations increase the risk to the insurgents using cyberspace and illuminate their supporting actors. Denying their anonymity, taking away their "free pass" and creating active operational effects is an important component in this fight. U.S. Cyber Command (USCYBERCOM) support must be deployed in a responsive, compact organization, be granted the authority to decide and act as required by the operational commander they support and be equipped with decentralized, preapproved action capability at the theater and regional command levels. There cannot be a complicated system controlling all effects produced by cyberspace capabilities; rather, cyber operations and effects need to be timely, streamlined and assured by responsive teams. U.S. forces must have the ability to decide quickly on the time and place for use of cyber capabilities to disrupt, deny, degrade or destroy an enemy's capacity to generate combat power in the physical or digital realm. A cyber-based "fires net" concept will lead to this capability.[17]

General Gary Luck, U.S. Army Retired, and Colonel Mike Findlay, U.S. Army Retired, developed a concept to demonstrate this framework.[18] Leaders' main concerns about any approval process often center on the amount of time it takes for a decision to be made. Tactical advantages in exploiting emerging opportunities are inherently linked to time; the longer it takes to make a decision, the more quickly the advantage is lost. Decentralizing the approval level and collaborating horizontally in a shorter time span (faster action cycles) will support commanders in achieving a tactical advantage. Figure 1 on the following page depicts the relationships between decision and action.

In particular, USCYBERCOM must be able to conduct CNA and CNE against targets on the Joint Effects List to disrupt insurgent network operations both in Afghanistan and globally.[20] Cyberspace operations should take a global offensive posture to reduce the effectiveness of insurgent finances, propaganda and command and control efforts. Additionally, USCYBERCOM should target individuals deemed to be negative influences, directly and indirectly, in order to support ISAF and United States Forces–Afghanistan non-kinetic operations. Creation of capacity to support cyberspace operations requires the design and establishment of a robust cyber support element, creation of an independent expeditionary cyberspace element located in Afghanistan and, finally, assigning to each U.S.-led regional command (RC) an increased digital network intelligence capability.

Recommendations for a Way Ahead

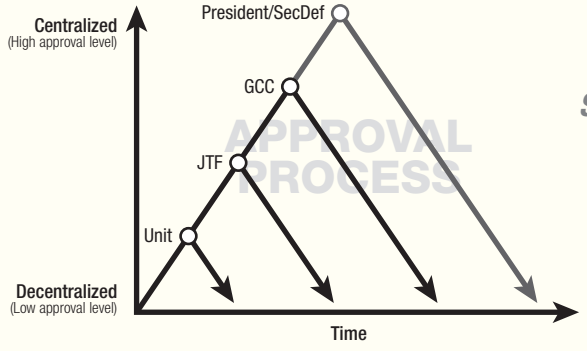
The agenda for implementing any significant change in current operations must start with a suitable framework that includes adherence to the laws affecting cyberspace operations, agency practices and theater organizational structures. None of these changes or amendments is simple or without risk. However, a total reexamination of how USCYBERCOM and the National Security Agency (NSA) conduct operations is required to ensure unity of effort and to manage efficiently the short supply of personnel and materials.

Cyberspace operations must be responsibly executed within legal titles and authorities contained in U.S. law; however, there seems to be an imbalance of evolution. The pace and direction of technological developments quicken each day, yet the laws that regulate these activities do not. The law must keep pace with technological developments to allow those planning and executing cyberspace operations the flexibility and agility required to accomplish their mission—to support warfighting commanders with integrated, synchronized cyber effects.

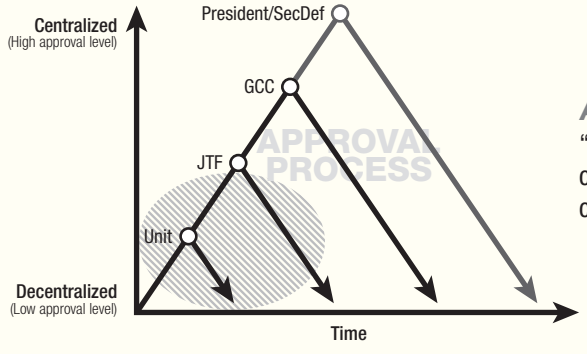
Figure 1

Decentralized Authority[19]

Mission Approval Levels

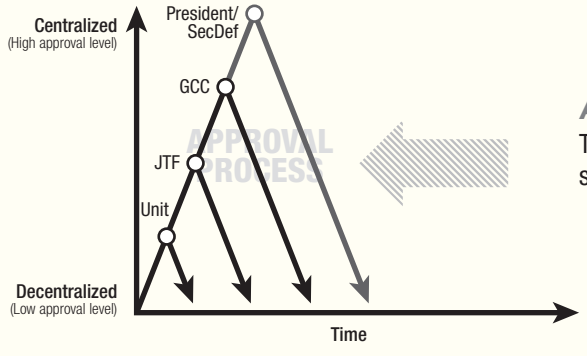


Standard Process



Alternate Method 1

"A priori" decisions, trust and confidence, and supported/ing command relationships solutions



Alternate Method 2

Technological and organizational solutions

Insights

- Delegate to the point of being "uncomfortably decentralized"
- Gain agility through horizontal collaboration
- Take advantage of emerging opportunities within chaos of battle

SecDef – Secretary of Defense GCC – Ground Component Commander JTF – Joint Task Force

U.S. Code Titles 10 and 50 define the roles and responsibilities of the armed forces and the intelligence community (IC), respectively.[21] Close cooperation and coordination would be required among USCYBERCOM, NSA and the greater IC to leverage their unique capabilities and authorities within defined legal restraints. While other members of the IC have a role in cyberspace operations, USCYBERCOM and NSA retain the dominant amount of personnel, capabilities and authorities. The relationship between these two organizations will largely dictate how cyberspace operations are conducted. Differences in titles and authorities between organizations are not an insurmountable obstacle. The obstacle will be changing the cultures and operational interaction between organizations in a way that allows them to collaborate within the framework of their legal authorities.

USCYBERCOM should consider creating a continental United States (CONUS)-based support cell called the USCYBERCOM CONUS Support Element, dedicated to providing continuous intelligence, technical and legal support to deployed CNO elements. This organization must be staffed with military and civilian intelligence officers capable of providing a wide range of timely support—including intelligence, research, legal review and interagency coordination—to deployed personnel. The authority to act autonomously within defined operational parameters is critical to allow the full range of cyberspace support.

As depicted in figure 2, forward-deployed elements must receive unified, agile and timely support from all cyber operations stakeholders.

Expeditionary Cyber Operations. In any conflict, intelligence enables operations. This concept also holds true for cyberspace operations. The USCYBERCOM CONUS Support Element must collect, process and analyze data for rapid delivery to expeditionary cyberspace support elements. This type of support requires intelligence analysts to perform both technical and traditional analysis continuously because there is no "off switch" for the Internet. Time zones do not apply and many interactions are asynchronous. Analysts must pay significant attention to their collection strategy and the sensitive operations they support.

To make the operational and RC-level cyber support elements more effective, they must develop greater capabilities and operational reach. Therefore, USCYBERCOM should develop a Theater Cyber Support Element–Afghanistan concept. This enhanced organization would have expanded authorities and capabilities to be leveraged at the direction of theater leadership under coordinated Title 10 and Title 50 authorities. The following serves as a potential model for future cyber COIN operations, theater/combatant command and joint task force/regional commands.

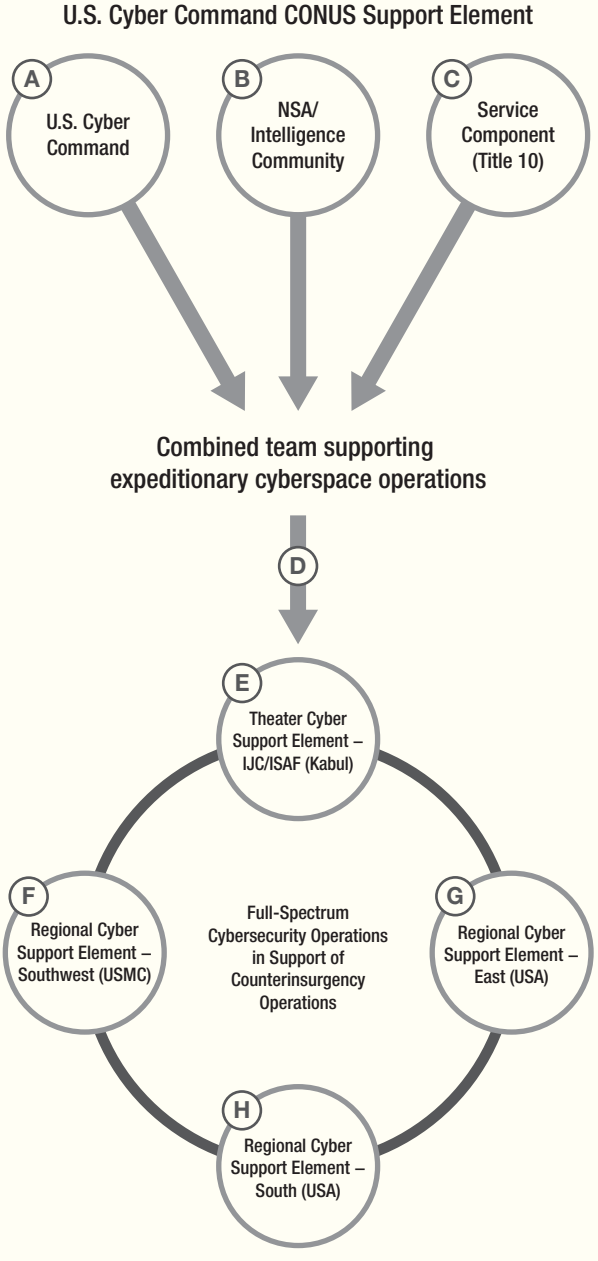
The Theater Cyber Support Element–Afghanistan would be leveraged to increase cyberspace operations supporting operational objectives outlined by the Commander ISAF and executed by RC teams. This commander must have the ability to effectively direct cyberspace operations in his battlespace. Additionally, he must be able to conduct cyberspace operations outside of his physical battlespace if cyber-based entities have a negative impact on his OE or ability to achieve his operational objectives. The cyber component of his enemy has no physical boundaries or territory.

USCYBERCOM's goal should be to enhance kinetic and non-kinetic operations in support of military information support operations, information operations, targeting and conventional intelligence operations.

The primary mission of the Theater Cyber Support Element–Afghanistan would encompass three distinct areas. First, this organization needs the ability to proactively and reactively

Figure 2

Proposed Organizational Relationship Between U.S. Cyber Command and the International Security Assistance Force



CNA – Computer Network Attack
CND – Computer Network Defense
CNE – Computer Network Exploitation
CO – Cyber Operations
CONUS – Continental United States
IAD – Information Assurance Directorate
IJC – International Joint Command
ISAF – International Security Assistance Force
NSA – National Security Agency
OPT – Operational Planning Team
USA – United States Army
USMC – United States Marine Corps

A ***U.S. Cyber Command***
- Staff Sections (J-2/3/7/OPT)
- Funding
- Doctrine
- Research and Development
- Authorities

B ***National Security Agency/ Intelligence Community***
- Collection
- Research and Technology
- Others as required

C ***Service Component (Title 10)***
- Personnel
- Funding
- Training

D ***Supports Theater Cyber Support Element***
- CNE used to develop meaningful intelligence supporting counterinsurgency operations
- CNA directed by command in theater of war
- CND support via IAD

E ***Theater Cyber Support Element – IJC/ISAF (Kabul)***
- Directs CO in support of combatant commander
- Provided with authorities and capabilities
- Allocates resources
- Supports ISAF/U.S. Forces Afghanistan

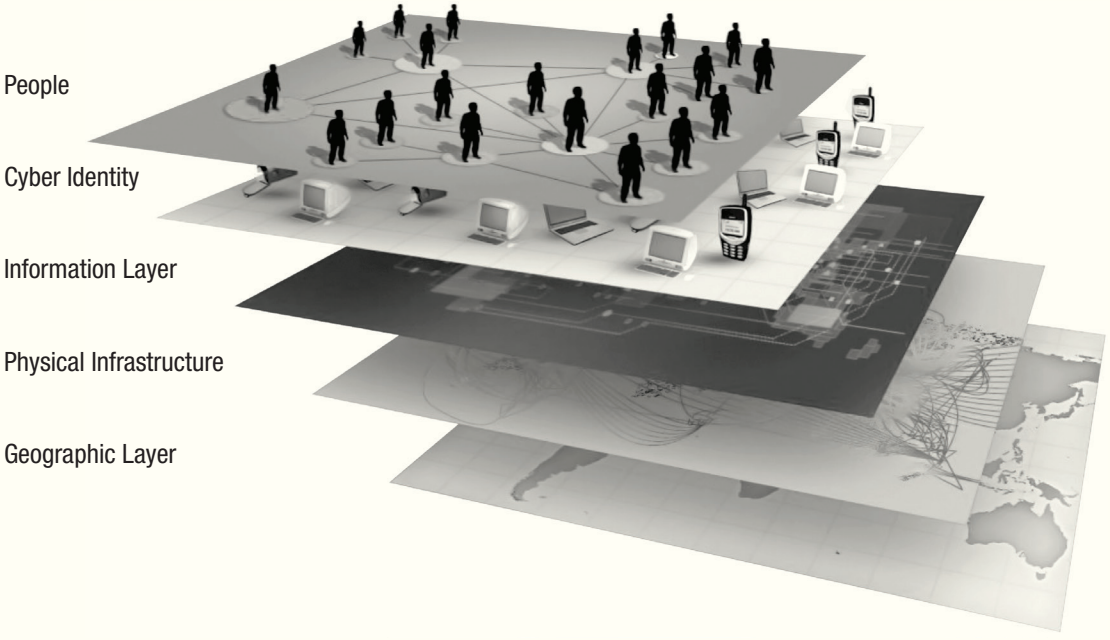
F ***Regional Cyber Support Element – Southwest (USMC)***
- Conducts research
- Identifies division targets
- Develops division targets
- Requests fires
- Supports division priorities

G ***Regional Cyber Support Element – East (USA)***
- Conducts research
- Identifies division targets
- Develops division targets
- Requests fires
- Supports division priorities

H ***Regional Cyber Support Element – South (USA)***
- Conducts research
- Identifies division targets
- Develops division targets
- Requests fires
- Supports division priorities

Figure 3

Relationship Between the Logical and Physical Environments[22]



counter insurgent propaganda. This could be support to IO or offensive cyber operations. Second, cyberspace operations could include the pursuit of insurgents and/or hierarchical structure in both cyber and physical domains. CNO should be fully integrated with the targeting process to develop a more complete picture of insurgents' networks (personalities, finances, relationships, etc.). While some of this integration does occur on a limited basis, it generally happens only at the national level and is insufficient to serve operational and tactical commanders across the scope of their mission. Finally, the USCYBERCOM Theater Cyber Support Element–Afghanistan should establish cooperation with NSA's Information Assurance Directorate to U.S. military communications providers. This relationship would provide RCs with access to an additional pool of CND expertise.

This enhancement to cyberspace operations could be achieved through relevant, measurable, responsive and properly resourced actions. The structure of the Theater Cyber Support Element–Afghanistan would require specially trained individuals to perform a range of duties. Among the most important personnel requirements is assignment of digital network intelligence analysts and CNO planners. Theater-level cyberspace operations would require a significant amount of coordination with RCs. RC cyberspace planning cells would become the conduit for information flow from the tactical level to the operational level.

RC cyberspace planning cells should be focused at the tactical level, targeting insurgents and their networks. These cells must plan cyberspace operations supporting tactical objectives outlined by regional commands. The senior military commander in an RC must be able to request cyberspace operations in his battlespace to shape kinetic, non-kinetic or intelligence operations in a timely fashion. As cyber operations are simply another tool, the commander must be able to synchronize tactical and operational cyber effects with the other tools and

operations he directs. To make major gains, cyber operations must be postured for speed and clearly demonstrate relevance to the regional commander.

RC cyberspace planning cells should consist of a basic CNO planning team capable of conducting independent research to develop and nominate targets. At a minimum, RC-focused cyber support should include Digital Network Intelligence and Dialed Number Recognition analysts, an all-source intelligence analyst and access to all required network connections and tools used to conduct digital network analysis. With this level of staffing and resources, the RC cyber support teams would be capable of conducting full-spectrum target analysis and transmitting that information to the theater cyber support element for action. All prioritization and deconfliction would take place in theater to rapidly execute operations in support of ISAF command priorities and RC operational and tactical requirements.

An Existing Model for Consideration. The signals intelligence (SIGINT) community support to combat operations presents a viable model for USCYBERCOM to provide commanders with a responsive and deployable operational cyberspace capability. Through this organization, the IC provides expeditionary cryptologic intelligence support from the combatant commander down to the division and brigade combat team levels in Afghanistan. This is accomplished through a tiered support structure that delegates authorities and responsibilities to SIGINT organizations within theater for specific mission areas. This concept of support provides commanders with responsive and focused intelligence capabilities in a manner applicable to future operational cyberspace support.

Expeditionary cyberspace operations and SIGINT have similar operational goals and analytical tools. Both strive to provide support down to the lowest level of combat operations and leverage national intelligence capabilities in a manner consistent with U.S. law to achieve forward deployed forces' operational objectives. The SIGINT model of support is mature and well tested and has the confidence of military commanders; it is a template for cyberspace forces to build future policies and procedures and to determine personnel composition based on a structurally sound frame.

Conclusion

It is of vital importance that the U.S. cyber and warfighting communities be fully aware of the increasing role that cyberspace operations can play in Afghanistan. This paper advocates an expanded approach in providing authority and structure to the senior and regional commands in Afghanistan, as well as integrating a more robust Cyber IPB effort on the part of the broader headquarters' planning and operational efforts. This paper offers a usable template for the future organizational structures required to enhance current efforts. The challenges presented are not difficult to overcome, but the will to change the status quo and embrace a different perspective is necessary. The agencies and commands involved in supporting combat operations have different cultures and methods of conducting operations. Some organizations are responsible for conducting intelligence operations while others are responsible for creating effects that support strategic objectives. The common bond between them is that the sum of their actions provides a tangible effect on the mission and supports the warfighter.

Endnotes

[1] General James E. Cartwright, Vice Chairman, Joint Chiefs of Staff, "Definition of Cyberspace Operations," action memorandum for Deputy Secretary of Defense, Washington, DC, 29 September 2008.

[2] Department of Defense, Joint Publication (JP) 3-13, *Information Operations* (Washington, DC: Department of Defense, 13 February 2006), http://www.carlisle.army.mil/DIME/documents/jp3_13.pdf.

[3] *Ibid*., p. GL-5

[4] *Ibid*., p. GL-6

[5] *Ibid*., p. GL-5

[6] Ian Simpson, "Afghanistan sees move to 3G in 2011," *Reuters Online*, 23 November 2010, https://uk.reuters.com/article/2010/11/23/oukin-uk-afghanistan-telecoms-idUKTRE6AM3PT20101123; Afghanistan Government Minister Baryalai Hassam (Deputy Minister Technical) stated that the Afghan Telecom Ministry is in negotiations with Afghan telecommunications companies to upgrade services to 3G and is intent on eventually upgrading to 4G services.

[7] Ekaterina Stepanova, "The Role of Information Communication Technologies in the Arab Spring: Implications Beyond the Region," Policy Memo No. 159 (Washington, DC: The Program on New Approaches to Research and Security in Eurasia, May 2011); during the uprisings throughout the Middle East (particularly Tunisia and Egypt), also known as the "Arab Spring," information technology played a substantial role in contributing to the coordination efforts of protestors. Websites such as Facebook and Twitter, various blogs and the use of text messages were all enablers for communications between various members of protest groups.

[8] As shown in June 2012 research conducted by the International Telecommunication Union, "Internet Users by Country," and Internet World Stats: Usage and Population Statistics, "Internet Users in Asia"; as of 30 June 2011, it is estimated that approximately 3.5 percent of Afghanistan's population have access to the Internet. This assessment is defined by fixed or wired broadband Internet subscriptions. The world average is 28.8 percent. See http://www.internetworldstats.com.stats3.htm and http://www.gfmag.com/tools/global-database/ne-data/10287-internet-users-by-country.html.

[9] Afghanistan Ministry of Communication & Information Technology, 9 February 2012, http://mcit.gov.af/en/page/12.

[10] See "Afghanistan National Development Strategy: Prioritization and Implementation Plan," Kabul International Conference on Afghanistan, 20 July 2012, p. 85, http://www.afghaneic.org/library/other/ANDS/ANDS-%20Prioritization%20and%20Imaplementation%20Plan%20Volume%20II.pdf.

[11] Scott Kirsner, "The Legend of Bob Metcalfe," *Wired*, vol. 6, no. 11, November 1988, http://www.wired.com/wired/archive/6.11/metcalfe_pr.html; Dr. Robert Metcalfe's Network Law: "The value of a network grows as the square of the number of its users. Or, more plainly stated: The more users who can talk to each other on a network, the more valuable it is."

[12] Margaret Rouse, "SearchMobileComputing: GPRS (General Packet Radio Services)," last modified May 2007, http://searchmobilecomputing.techtarget.com/definition/GPRS; both 3G and GPRS provide a faster data rate to users than GSM, which is the primary communications protocol used in cellular communications in Afghanistan.

[13] Department of Defense, JP 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: Department of the Army, 20 March 2006).

[14] *Ibid*.

[15] Department of the Army, Field Manual (FM) 1-02, *Operational Terms and Graphics*, 21 September 2004, p. 1-102.

[16] Department of the Army, FM 3-24/Marine Corps Warfighting Publication 3-33.5, *Counterinsurgency*, 15 December 2006.

[17] Department of the Army, U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-3-4, *The U.S. Army Functional Concept for Fires 2016–2028*, 13 October 2010, p. 35; a fires net "provides assured communications, capacity and timeliness to expedite the clearance and execution of offensive and defensive fires."

[18] General Gary Luck (USA Ret.) and Colonel Mike Finley (USA Ret.), "Joint Operations, Insights and Best Practices," 2nd ed. (Norfolk, VA: Joint Warfighting Center, July 2008), http://www.au.af.mil/au/awc/awcgate/jfcom/joint_ops_insights_july_2008.pdf.

[19] *Ibid*., p. 47.

[20] Joint Effects List (JEL) is not a doctrinal term contained in official Army doctrine (FM 1-02, *Operational Terms and Graphics*, September 2004). However, it is widely accepted as a valid doctrinal term and concept used for targeting within forward deployed military organizations.

[21] House of Representatives, Committee on Armed Services, Title 10, *United States Code Armed Forces* (Washington, DC: U.S. Government Printing Office, July 2011), http://armedservices.house.gov/index.cfm/files/serve?File_id=fc0173d5-f7d3-4d74-8d42-1b9e185b7c6b; Title 50, *War and National Defense,* http://uscode.house.gov/pdf/2011/2011usc50.pdf.

[22] Department of the Army, TRADOC Pamphlet 535-7-8, *Cyberspace Operations Concept Capability Plan 2016–2028*, 22 February 2010, p. 8.

Glossary

CDMA	Code Division Multiple Access
CIPB	Cyber Intelligence Preparation of the Battlespace
CNA	Computer Network Attack
CNE	Computer Network Exploitation
CND	Computer Network Defense
CO	Cyber Operations
COIN	Counterinsurgency
CONUS	Continental United States
FM	Field Manual
GCC	Ground Component Commander
GIROA	Government of the Islamic Republic of Afghanistan
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communication
IAD	Information Assurance Directorate
IC	Intelligence Community
IJC	International Joint Command
IO	Information Operations
IPB	Intelligence Preparation of the Battlespace
ISAF	International Security Assistance Force
JEL	Joint Effects List
JP	Joint Publication
JTF	Joint Task Force
MCIT	Ministry of Communications and Information Technology
NSA	National Security Agency
OE	Operational Environment
OPT	Operational Planning Team
RC	Regional Command
SecDef	Secretary of Defense
SIGINT	Signals Intelligence
TRADOC	U.S. Army Training and Doctrine Command
USA	United States Army
USCYBERCOM	United States Cyber Command
USMC	United States Marine Corps