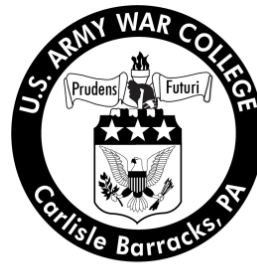


Unconventional Warfare in Cyberspace

by

Colonel Everett Denton Knapp, Junior
United States Army



United States Army War College
Class of 2012

DISTRIBUTION STATEMENT: A

Approved for Public Release
Distribution is Unlimited

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 03-22-2012		2. REPORT TYPE Strategy Research Project		3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE Unconventional Warfare in Cyberspace				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Colonel Everett Denton Knapp, Junior				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)				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					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT Current and potential adversaries of the United States and its allies have made use of the internet to coerce, disrupt, or overthrow competing groups, regimes, and governments in their own unconventional warfare strategies. Although the national and defense strategies now emphasize operations in Cyberspace, most of the focus is defensive, rather than offensive. The United States Special Operations Forces (SOF) are inadequately postured to conduct Unconventional Warfare (UW) in and through the Cyberspace Domain as part of the full range of Special Operations. This paper specifically focuses on the capabilities required for SOF to conduct Unconventional Warfare in and through the Cyberspace Domain in support of Combatant Commands. It will address the current conceptual and doctrinal documents, as well as policies and authorities for UW in Cyberspace; describe SOF in Cyberspace in the context of the seven phases of UW, and finally address the unclassified capability shortfalls and potential solutions utilizing the Doctrine, Organization, Training, Materiel, Leadership and Education, Facilities, and Policy (DOTMLPF-P) framework.					
15. SUBJECT TERMS Irregular, Cyber, Social Media, Special Operations, Special Forces					
16. SECURITY CLASSIFICATION OF: UNCLASSIFIED			17. LIMITATION OF ABSTRACT UNLIMITED	18. NUMBER OF PAGES 36	19a. NAME OF RESPONSIBLE PERSON
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED			19b. TELEPHONE NUMBER (include area code)

USAWC STRATEGY RESEARCH PROJECT

UNCONVENTIONAL WARFARE IN CYBERSPACE

by

Colonel Everett Denton Knapp, Junior
United States Army

William O. Waddell
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

The views expressed in this student academic research paper are those of the author and do not reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

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

ABSTRACT

AUTHOR: Colonel Everett Denton Knapp, Junior
TITLE: Unconventional Warfare in Cyberspace
FORMAT: Strategy Research Project
DATE: 22 March 2012 WORD COUNT: 6,980 PAGES: 36
KEY TERMS: Irregular, Cyber, Social Media, Special Operations, Special Forces
CLASSIFICATION: Unclassified

Current and potential adversaries of the United States and its allies have made use of the internet to coerce, disrupt, or overthrow competing groups, regimes, and governments in their own unconventional warfare strategies. Although the national and defense strategies now emphasize operations in Cyberspace, most of the focus is defensive, rather than offensive. The United States Special Operations Forces (SOF) are inadequately postured to conduct Unconventional Warfare (UW) in and through the Cyberspace Domain as part of the full range of Special Operations. This paper specifically focuses on the capabilities required for SOF to conduct Unconventional Warfare in and through the Cyberspace Domain in support of Combatant Commands. It will address the current conceptual and doctrinal documents, as well as policies and authorities for UW in Cyberspace; describe SOF in Cyberspace in the context of the seven phases of UW, and finally address the unclassified capability shortfalls and potential solutions utilizing the Doctrine, Organization, Training, Materiel, Leadership and Education, Facilities, and Policy (DOTMLPF-P) framework.

UNCONVENTIONAL WARFARE IN CYBERSPACE

This conflict has extended into the cyber arena. We have adapted to changes in the traditional forms of conflict, but we are not yet adequately prepared for this contest.

—General Martin Dempsey¹

As the fifth and recently emerging domain within the strategic operational environment, Cyberspace has gained the attention and prioritization of the National Command Authority and Department of Defense. Current and potential adversaries of the United States and its allies have made use of the internet to coerce, disrupt, or overthrow competing groups, regimes, and governments in their own unconventional warfare strategies. As the DoD proponent for special operations, the United States Special Operations Command is exploring Special Operations Forces' current and future capabilities within the Cyberspace Domain. As Special Operations Forces examine their ability to execute core missions across every domain, leaders must take an internal look at skills and expertise that have degraded after a decade of conflict in the Middle East. Unconventional Warfare (UW) is one of the core missions that the Special Operations community has not trained or executed with consistency over the past years, and is now faced with a greater challenge of executing Unconventional Warfare in the new Cyberspace domain.

Military Problem

The United States' Special Operations Forces are inadequately postured to conduct Unconventional Warfare in and through the Cyberspace Domain as part of the full range of Special Operations. This paper specifically focuses on the capabilities required for Special Operations Forces to conduct Unconventional Warfare in and

through the Cyberspace Domain in support of Combatant Commands. Specifically, it will address the current conceptual and doctrinal publications, as well as policies and authorities for Unconventional Warfare and Cyberspace; describe Special Operations Forces in Cyberspace in the context of the Seven Phases of Unconventional Warfare; and finally address the unclassified capability shortfalls and potential solutions utilizing the Doctrine, Organization, Training, Materiel, Leadership and Education, Facilities, and Policy (DOTMLPF-P) framework for future changes.

The exponential growth of Cyberspace has changed the dynamics of the joint operating environment in ways futurists have only begun to imagine. In just the span of a decade, the use of social media through the internet became a catalyst for such significant events as the the Arab Spring phenomenon and the world-wide protest of the Columbian Revolutionary Armed Forces of Colombia (FARQ) narcotics group². Al Qaeda continues to recruit, train, and terrorize using the internet to reach out from hidden safe havens. The ability to gain almost perfect knowledge on an individual's or group's demographics and networks is near instantaneous. Potential and actual adversarial state and non-state actors make it a priority to use this technology to influence relevant populations. As the United States explores the potential shortfalls in its cyber strategy, time is critical, as adversaries may reach parity or dominance in their cyber capabilities to challenge the U.S. and its allies at home and abroad.

The technological capability for the United States military to operate in this new domain exists, and recent advances in authorities, doctrine, training, equipping and execution limit enemy infiltration of computer networks; however, the will and authority to implement offensive cyber options fall far behind those of our potential adversaries.

Most of the national-level strategies, as well as those of the Department of Defense and services focus on computer and network defense capabilities. Most cyberspace directives and doctrine only address hardware and systems security. An offensive approach would provide a means to apply technological advances in areas such as networked social media on the Internet to enhance the capabilities of Special Operations Forces to conduct Unconventional Warfare in support of the nation, Joint Force and Combatant Commands.

The Threat Operating in Cyberspace

Today, the most common type of threat comes from groups that wage war from the shadows, using the basic precepts of guerrilla warfare. They understand that the only way to defeat a larger, stronger enemy is to use unconventional tactics, and recent activities indicate their effective use of the cyberspace domain.³ As the national and defense strategies continue to focus on defensive network measures to defeat this threat, the risk of neglecting our own offensive capabilities increases exponentially.

Adversaries of the United States are effectively using their own forms of Unconventional Warfare in the U.S. to recruit and terrorize from within. Al Qaeda has done this very effectively in recent years. Al-Shabaab in Somalia and Sudan connect online with young men in the United States.⁴ The U.S. threat in Cyberspace includes Americans who travel overseas to the tribal areas of Pakistan, Yemen, or Africa for hands-on training, and then return to the United States. The threat also includes Americans radicalized in their own homes through chat rooms on the Web, finding like-minded people. The enemy can be overseas, or the next-door neighbor.⁵

Background for Unconventional Warfare in Cyberspace

U.S. Special Operations Command, U.S. Joint Forces Command, and representatives from the Joint and Interagency communities developed the Irregular Warfare Joint Operating Concept. The capability based assessments that followed led to the development of three Joint Integrating Concepts, including the Unconventional Warfare Joint Integrating Concept (UW JIC), which identified many specific capability shortfalls related to Unconventional Warfare in the Cyber Domain; however, this paper will only address the unclassified capability shortfalls and potential solutions.

The Unconventional Warfare Joint Integrating Concept recommends developing or improving tactics, techniques, and procedures for conducting and supporting Unconventional Warfare in urban environments and with cyber tools. It identifies the use of Cyberspace to develop capabilities that will support long-term Unconventional Warfare activities, provide access to denied populations, and mitigate risks involved in placing personnel in hostile, denied areas for extended periods.⁶

In 2009, the United States Special Operations Command formed an Integrated Project Team Working Group to explore the enabling of Special Operations using Cyberspace, and primarily focused on Unconventional Warfare and Preparation of the Environment. The Cyberspace Front End Assessment conducted by USSOCOM focused on 4 specific areas: Cyber Training and Skills; Tactical Cyber Operations; Tactical Cyber Capabilities, and Insider Threat Mitigation. In 2011, USSOCOM expanded its efforts to broaden the scope of the concept to “Special Operations in and through the Cyberspace Domain (SOCD)”.⁷ SOCD is still under conceptual development, and focuses on a macro-look at Special Operations within the

Cyberspace Domain. This paper will focus more specifically on the U.S. Army's Special Forces' capabilities to conduct Unconventional Warfare in Cyberspace.

The United States Army Special Operations Command has placed increased emphasis on Special Forces' ability to conduct Unconventional Warfare as a core mission. Many leaders within the Special Operations community believe that Special Forces operators have lost critical skill sets to conduct Unconventional Warfare due to the demands for Direct Action missions during the last ten years of conflict in the Middle East. Very few Special Forces operators have conducted Unconventional Warfare, and for those that have, it has been a very long time. Although case studies point out that the Special Forces operations with the Northern Alliance in Afghanistan constituted unconventional warfare, the preparedness and expertise of operators to conduct this Unconventional Warfare was debatable. Since 2009, service-specific, as well as joint doctrine has revised the definition and other aspects of UW, and captured it in new manuals and programs.

The Joint Staff, USSOCOM, and the Army published conceptual and doctrinal definitions for both Unconventional Warfare and Cyberspace within the last two years. Unconventional Warfare is defined as activities conducted to enable a resistance movement or insurgency to coerce, disrupt, or overthrow a government or occupying power by operating through or with an underground, auxiliary and guerilla force in a denied area.⁸

The Department of Defense defines Cyberspace as a global domain within the information environment consisting of the interdependent network of information technology infrastructures including the Internet, telecommunications networks,

computer systems, and embedded processors and controllers.⁹ The 2010 Quadrennial Defense Review states that although cyberspace is a man-made domain, it is now as relevant a domain for Department of Defense activities as the naturally occurring domains of land, sea, air, and space.¹⁰ Recent national, departmental, combatant command, and service strategies all mention cyber and cyberspace in some form within their documents.

With the realization that the new strategic environment has potential adversaries that currently use the cyber domain without moral, legal, or technological constraints or limitations, national and military leaders rapidly provided guidance to move the joint force into the cyber domain. With the proliferation of state and non-state actors conducting irregular warfare, and the deep cuts in U.S. defense spending, the focus towards a smaller, but more capable force is driving very specific missions and priorities. Unconventional Warfare, a component of Irregular Warfare, is a critical means to accomplish stated missions in the Defense Strategic Guidance.

Strategic Guidance

The new Defense Strategic Guidance (January 2012) lists ten primary missions of the Armed Forces. Of the ten missions, “Counter Terrorism and Irregular Warfare”, and “Operate Effectively in Cyberspace and Space” directly relate to the conduct of unconventional warfare in Cyberspace. In his opening letter in the Defense Strategic Guidance, President Barrack Obama focused on the use of new technologies, specifically Cyberspace. He mentioned Special Operations and engagement with allies; counterterrorism; operating in anti-access environments; and prevailing in all domains, including cyber. The Secretary of Defense added to the guidance by addressing sustainment of technological and networked advantages, the importance of the

military's capability to project power, and operating in cyberspace to defeat al-Qaeda and its affiliates.¹¹

The Defense Strategic Guidance directs active countering of threats by monitoring non-state threat activities, working with allies and partners to control ungoverned places, and directly attacking dangerous individuals and groups. To support these objectives, the U.S. must place priority on military and allied presence within designated countries, and the support of partner nations in the region. This support may come in the form of unconventional warfare conducted by the U.S. within those nations.

The following paragraphs discuss how UW in Cyberspace can apply specifically to the directed missions within the Defense Strategic Guidance. In addressing the first and most relevant mission, "Counter Terrorism and Irregular Warfare," the Defense Strategic Guidance states that U.S. military forces must act in concert with other means of national power to hold al-Qaeda and its affiliates under constant pressure. As U.S. forces draw down in Afghanistan, our global counter terrorism efforts will become more widely distributed and characterized by a mix of direct action and security force assistance. The U.S. military must continue to build and sustain tailored capabilities for counter terrorism and irregular warfare, and remain vigilant to threats posed by terrorist organizations.¹²

The directed mission of "Deter and Defeat Aggression" by any potential adversary requires the U.S. forces to deny a capable state's aggressive objectives in one region by conducting a combined arms campaign across all domains – land, air, maritime, space and cyberspace. This includes the ability to secure territory and populations, and facilitate a transition to a stable governance on a small scale for a

limited period using a standing force and an extended period with mobilized forces. U.S. forces committed to a large-scale operation in one region, must be capable of denying the objectives of, or imposing unacceptable costs on, an opportunistic aggressor in a second region. U.S. forces will operate with allied and coalition forces, and ground forces will be responsive and capitalize on balanced lift, presence, and prepositioning to maintain the agility needed to remain prepared for the several areas in which such conflicts could occur. The use of UW in the Cyber domain provides a means to achieve presence and prepositioning for long periods of time, operating by, with and through indigenous forces in one area, while also providing support to a major contingency.¹³

“Project Power Despite Anti-Access/Area Denial Challenges” is a mission that directly relates to the use of Unconventional Warfare to gain access to denied areas, while keeping a small, low cost footprint. Both state and non-state actors threaten access and possess the capability and intent to conduct cyber espionage and cyber attacks with possible severe effects.¹⁴ In order to credibly deter potential adversaries and to prevent them from achieving their objectives, the U.S. must maintain its ability to project power in areas of limited or denied access. Adversaries will use asymmetric capabilities, including electronic and cyber warfare and other methods to complicate operations. The U.S. military must continue to invest to ensure its ability to operate effectively in anti-access and area denial environments, including implementation of the Joint Operational Access Concept.¹⁵

The mission of “Operate Effectively in Cyberspace and Space” states that modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and

space. DoD must continue to work with domestic and international allies and partners and invest in advanced capabilities to defend its networks, operational capability, and resiliency in cyberspace and space.¹⁶ The mission description does not mention the use of offensive capabilities within Cyberspace.

The mission of “Conduct Stability and Counterinsurgency Operations” must emphasize non-military means and military-to-military cooperation to address instability and reduce the demand for significant U.S. force commitments to stability operations. U.S. forces will retain and continue to refine the lessons learned, expertise, and specialized capabilities developed over the past ten years of counterinsurgency and stability operations. Since U.S. forces will no longer be sized to conduct large-scale, prolonged stability operations, the military must examine how this strategy will influence existing campaign and contingency plans, to place limited resources against mission requirements. This will include a renewed emphasis on the need for a globally networked approach to deterrence and warfare.¹⁷ The use of Special Operations Forces utilizing this approach in Cyberspace is a means to accomplish this stability.

Most of the national-level strategies, as well as those of the Department of Defense and service-levels focus on computer and network defense capabilities. Current Cyberspace directives and doctrine only address hardware and system security. What about an offensive strategy? An offensive approach provides a means to apply technological advances in networked social media on internet and cellular devices to enhance the capabilities of Special Operations Forces to conduct Unconventional Warfare in support of the combatant commanders’ theater campaign plans over a long

duration. The current shortfalls will only exponentially increase in the future, if change is not initiated and accelerated to keep up with potential adversaries.

The Secretary of the Army published his top priorities on February 14, 2012, listing “Strengthen information assurance and cybersecurity” as his number seven priority. However, this priority is focused on assuring the availability, confidentiality, and integrity of information and the systems that process, store, and transmit information. It focuses on the risk of not meeting information assurance standards or leaving exposed cybersecurity weaknesses.¹⁸ However, once again, the focus is on defense of systems.

Guidance for the Conduct of Unconventional Warfare in Cyberspace

In February 2011, USSOCOM developed a working definition of “Special Operations Conducted Using the Cyberspace Domain.” The group defined it as operations conducted in and through Cyberspace to execute special operations. This includes Special Operations conducted to support Cyberspace operations, which may be conducted unilaterally or through, with, or by allies, host nation, indigenous and surrogate forces, and may vary in length from short-term to long-term engagements.¹⁹

In recent Irregular Warfare concepts, the phrase, “it takes a network to defeat a network”, supports the capability of Special Operations Forces in an Unconventional Warfare campaign to identify both friendly and adversary networks. President Barack Obama stated in his guidance, that as the nation transitions out of Iraq and draws down in Afghanistan, it must take extra measures to retain and build on key advancements in networked warfare in which joint forces have finally become truly independent. This imperative will shape a number of Departmental disciplines.²⁰ In particular, the Departments of Defense and State must work together toward this end by taking into account the need for Special Operations Forces to regain proficiency in Unconventional

Warfare, and once again place emphasis on its use within a Combatant Commander's arsenal of irregular capabilities to counter the irregularly networked adversaries within Cyberspace.

As specified in the Defense Strategic Guidance by the Secretary of Defense, similar work needs done to ensure the U.S., along with its allies and partners are capable of operating in Anti-Access and Area Denial (A2/AD), cyber, and other contested operating environments. The military must maintain the imperative to sustain key streams of innovation that may provide significant long-term payoffs. With the reduction in budget, the Defense Strategic Guidance stresses the protection of the investments in Special Operations Forces, as well as new technologies such as space and Cyberspace capabilities.²¹ To conduct Cyber War effectively, the future force requires improved and new capabilities. Access is the first and most critical requirement for Cyber War capabilities and is therefore a major point of emphasis in the required capabilities.²² Access requires early engagement with individuals and groups within specified nations and their surrounding neighbors to assist in shaping the environment for access prior to offensive action. Offensive warfare by Internet must adapt offensive warfare theory to the peculiarities of the Internet and to the nature and aims of the parties in conflict.²³

The Chairman of the Joint Chiefs of Staff specifically addressed cyber multiple times in his Strategic Direction to the Joint Force. He emphasized that the military must prevent and mitigate a cyber attack, and extend cyber domain awareness, establish an active defense, and provide responsible offensive capabilities. Networked special operations, cyber and Intelligence, Surveillance, and Reconnaissance (ISR) will become

increasingly central.²⁴ The joint force must find new ways to combine and employ emergent capabilities such as cyber, special forces, and ISR, and move towards Joint information and simulation networks that support secure and agile command and control.²⁵ This is the first strategic document to cite the need for offensive capabilities in the Cyberspace Domain.

In his March 6, 2012 Posture Statement to the Congress Senate Armed Services Committee, Admiral William H. McRaven, Commander, U.S. Special Operations Command, stated that

strategic trends and challenges are producing a distinct change of character of conflict. Insurgents, transnational terrorists, criminal organizations, nation states and their proxies exploit gaps in policy developed for the more predictable world of yesterday. Increasingly these threats are networked, adaptable, and empowered by cyberspace to find new ways to recruit, train, finance, and operate. In short, the strategic environment is changing – quickly and constantly.²⁶

Both Unconventional Warfare and the Cyberspace Domain provide the Combatant Commanders with options for accomplishment of national military missions, while limiting the size of forces required, the operating costs, and the limited overt involvement in the operating environment.

Incorporating the Seven UW Phases Within the Cyberspace Domain

Joint and Army doctrine describe a U.S. – sponsored UW operation in seven phases. The Special Operations Forces' use of cyberspace in each of phase would enhance current capabilities and expand into new capabilities. The following paragraphs explore each phase of Unconventional Warfare, by explaining the phase, exploring possible implications for the phase in Cyberspace, and citing specific examples.

Phase One (Preparation). During Phase I, Special Operations Forces conduct intensive assessments of the target populations and regions to determine resistance potential, identify existing irregular forces and their leadership, and anticipate potential popular support for a resistance effort and likely enemy responses. Military Information Support Operations (MISO) also begin preparation within the region with the population and insurgents.²⁷

In the Cyberspace Domain, Special Operations Forces would conduct Cyber Intelligence Preparation of the Environment (CIPOE). Special Operations Forces operators can obtain an enormous amount of real-time information and insight into the identification of leaders, recruits, events, norms, and exploitable themes through the use of the internet and social networking. The internet provides an important access vehicle for supporting influence activities when target audiences reside in denied or limited access areas. This capability specifically enables one of the ten priority missions discussed in the Defense Strategic Guidance document, “Project Power Despite Anti-Access/Area Denial Challenges.”

For example, crowdmapping is one of the new social media trends that may assist operators during the Preparation Phase. Crowdmapping is similar to Twitter and Facebook, relying on user-generated videos, images, and reports. The Syria Tracker is another example of the successful use of a crowdmap to monitor and document Syrian detentions and protests. Syrian activists launched the map in May 2011 and have successfully documented over 800 instances of human rights abuses by the Syrian government. A similar crowdmap website created in 2008 geo-plotted reports of violence in Kenya following the country’s 2007 elections. Crowdmapping had an impact

in the Arab Spring, and this tool provides a new way to utilize the Internet and to achieve certain objectives.²⁸

Phase II (Initial Contact). The Initial Contact Phase is a critical and potentially the most dangerous phase of the Unconventional Warfare operation. Special Operations Forces Pilot Teams infiltrate the Joint Special Operations Area to make initial contact with an indigenous element. The team conducts a physical assessment of the situation, begins development of relationships, exfiltrates key indigenous personnel for training, and prepares for follow-on forces. Military Information Support Operations (MISO) intensify efforts to gain popular support for the insurgency and undermine the existing government's legitimacy.²⁹

Initial contact with resistance leadership through the internet could provide access early in the operation, exposing U.S. personnel to less risk. Operators could virtually initiate the establishment of relationships, provide early organization and training guidance, and plan for extraction of key resistance personnel. Use of the internet for initial contact would require development of small, easily down-loadable encryption capabilities to provide for secure communications between the U.S. and the indigenous insurgent elements.³⁰

An example of the adversary's use of Cyberspace is Osama bin Laden use of the internet to make contact with potential followers. One of his stated goals was the creation of an ideology that could go global. Al-Qaeda's Anwar Al-Awlaki was one of Osama bin Laden's key leaders, and through his blog, his online lectures, e-mail, and social networking sites, including Facebook, he reached thousands.³¹ Al Qaeda's

contact with possible recruits was done personally in the Middle East, but also online across the internet.³²

During the Initial Contact Phase, physical contact with indigenous elements is important to develop close interpersonal relationships and trust. However, in denied or controlled areas, Cyberspace may be the only viable way to make contact, and social networking within the domain provides another means to connect to these elements. Cyberspace may reduce some risk of compromise, but may increase the risk of disclosing involvement if detected. Cyberspace has the ability to be a strategic, operational, and tactical military enabler for Special Operations Forces Operators to reach indigenous forces in closed areas.³³

An example of an emerging capability within social media is business' use of Online Tracking, Tagging, and Locating (TTL) technology to identify potential markets down to individual-level. Approximately 99% of online users use Google and search engines to find information. The capability exists in current technology to locate keywords to identify target audiences through interest, category, and behavior based on their internet searches. Once a user is targeted, the operator can electronically follow the user through future internet usage and continue to target the user with customized messaging in real-time. Utilizing advanced Social Media Monitoring tools, operators have the capability to track not only targeted users, but also their online peers and those with similar online behavior.³⁴ Once the individual or group is retargeted as an ideal user, behavioral retargeting technology allows an operator to follow the user throughout future online activities. With 100% mobile penetration, mobile reach and targeting allows overlay of both online activity and location to target advertising.³⁵ Watching videos is

one of the most popular online activities in the Middle East, especially among young males, with millions of video views each day. This technology can also target alongside videos, with pre-roll, post-roll, and hover-advertising associated with videos watched.³⁶

Phase III (Infiltration). This phase involves the infiltration and link-up of follow-on personnel from the Special Forces Operational Detachment – Alpha (SFODA), supporting forces, and integration with the pilot team and indigenous insurgent groups. Civil-Military Operations (CMO) begin with Special Operations Forces support of the insurgency and supportive populations. Military Information Support Operations (MISO) continues, focusing on building local and regional support for the insurgency. During the Infiltration Phase, operators could communicate over the internet to provide instruction to widely dispersed insurgent groups, coordinate infiltration activities, and provide communication for infiltration synchronization. This also enables the infiltration teams to build rapport with their insurgency counterparts.³⁷

Phase IV (Organization). During the Organization Phase, Special Operations Forces organize and develop irregular forces, as well as establish internal and external support networks. Civil Military Operations activities support this infrastructure development and outreach efforts directed at the supporting population. Special Forces Operational Detachments - Alpha could employ Cyberspace communications to expand their range of influence, recruiting, and training with indigenous insurgents much earlier than previously possible, with lower risk of exposure in limited access areas. If properly secured and protected, blind communications could occur rapidly throughout the insurgent organization, as well as the general population. Virtual training of indigenous insurgents would allow operators time to concentrate on other critical mission areas.

The use of the internet to fund insurgents would reduce monetary transfer restrictions and tracing. The use of Cyberspace capabilities could support the development of procurement systems, sources of supply, and secure delivery mechanisms. A government in exile and resistance movements would have increased opportunities to build relationships and develop a unified effort.³⁸

Offensive capabilities in the military domain of Computer Network Operations may be used to disrupt, disable, degrade, or deceive an enemy's command and control, affecting his ability to make timely and effective decisions, while protecting and preserving the friendly command and control. Both Computer Network Attack (CNA) and Computer Network Exploitation (CNE) can enable Unconventional Warfare in this phase. Recent examples are the multiple network intrusions experienced by corporations, financial institutions, as well as the Pentagon within the United States by foreign adversaries.

Phase V (Buildup). During the Build Up Phase, expansion of insurgent forces and territory, advanced military training, and strengthening procurement and delivery systems to support larger insurgent activities over greater areas occurs. Military Information Support Operations personnel tailor themes to support the popular will of the people and the government in exile. The most significant Cyberspace capabilities include virtual training, transfer of funds, and the continued recruitment and support of the insurgency through the Internet. An example of this is the Department of Defense's Knowledge Online web-based training modules utilized by military personnel worldwide.³⁹

Phase VI (Employment). During the Employment Phase, insurgent combat operations increase against the government or occupation forces. As insurgent operations become more conventional, general purpose forces may be introduced and transition to open warfare. During this phase, the use of the Cyberspace Domain may enable critical command and control functions across guerrilla and regular forces. Digital communications and linked networks would facilitate rapid information sharing across forces and government agencies in support of the insurgency.⁴⁰

Phase VII (Transition). During the Transition Phase, once hostilities cease and the new government is re-established, the insurgents are disbanded and transitioned either to civilian status or incorporated into legitimate security forces. Military Support Operations and Civil Affairs support the transition, focus on building support for the new government, and assist civilian infrastructure reconstruction and improvement. The use of the internet would expedite the notification of security forces, as well as promulgate the strategic messages of the new government to the relevant population.⁴¹

The conduct of the seven phases of Unconventional Warfare by Special Forces personnel requires support from across the Joint Force and various government agencies. The capabilities needed to support operators in various domains continues to evolve with the changing strategic environment; however, much more change must take place to ensure the readiness of the Special Operations Forces in Cyberspace.

The Secretary of Defense, Leon E. Panetta, stated that the Department of Defense Fiscal Year 13 Budget would invest \$3.4 billion in cyber activities, and that the Department of Defense is investing in full spectrum cyber operations capabilities to address the current and future threats. The Department of Defense is also receiving

support through legislation addressing Cyberspace introduced by Senators Lieberman and Collins.⁴²

The Defense Advanced Research Projects Agency (DARPA) issued a new solicitation for innovative research proposals in social media in strategic communication for a new science of social networks built on an emerging technology base. DARPA anticipates \$42 million in support of fundamental research over the next three years. DARPA noted that operations are rapidly changing with the spread of blogs, social networking sites, and media-sharing technology, all further accelerated by mobile technology proliferation. Changes to the nature of conflict resulting from the use of social media are likely to be as profound as those resulting from previous communications revolutions. The effective use of social media has the potential to help the Armed Forces better understand the operating environment and allow more agile use of information.⁴³

The Social Media in Strategic Communications (SMISC) Program will develop a new science of social networks built on an emerging technology base, and develop automated and semi-automated operator support tools and techniques for the systematic and methodical use of social media at data scale and in a timely fashion to accomplish four specific program goals. These goals include detect, classify, measure and track the formation, development and spread of ideas and concepts; and purposeful or deceptive messaging and misinformation; recognize persuasion campaign structures and influence operations across social media sites and communities; identify participants and intent, and measure effects of persuasion campaigns; and counter messaging of detected adversary influence operations.⁴⁴

DOTMLPF-P Implications for UW in the Cyberspace Domain

The following paragraphs explain the unclassified capability gaps and recommendations for potential solutions across the spectrum of Doctrine; Organization; Training; Materiel; Leadership & Education; Personnel; Facilities; and Policy (DOTMLPF-P). The USSOCOM Integrated Project Team (IPT) conducted a front-end assessment of the current cyber status and future requirements. The group identified seven cyberspace capabilities required for SOF for the next 5-15 years, with 40 supporting tasks. Of the seven capabilities, three are classified and four are unclassified. Unclassified capabilities include leveraging technology to enhance execution of Special Operations missions; providing near real-time subject matter expert support through Cyberspace; interaction (operate) with Mission Partners/Partner Nations/Other Government Organizations/Non-government Organizations, and non-state actors within the Cyberspace Domain; and conduct Sensitive Site Exploitation.⁴⁵

Doctrine. The Joint Force and services continue to produce conceptual and doctrinal products to capture current lessons learned, as well as necessary capabilities for the Cyberspace Domain. The current doctrine for Cyberspace is focused predominantly on defense of computer networks. With the continued exponential growth of Cyberspace and its impact on governments, businesses, and society, it will fundamentally change how people learn, communicate, perceive, and interact. USSOCOM must address changes to reflect this new environment in its Tactics, Techniques, and Procedures (TTP) for executing missions.⁴⁶

The joint force should develop contingency operations, as well as conduct joint experimentation in support of concept and doctrine development, to gain an understanding of the potential for Unconventional Warfare as a strategic option for use

against both state and non-state actors within the Cyberspace Domain. An example of a potential venue for experimentation is the Information Operations (IO) Range, which would allow participants to wargame Cyberspace options within a future scenario to identify capability gaps and solutions. Potential tasks for exploration include developing potential resistance forces, recruiting, training, funding irregular forces, communicating with and among irregular forces, and coordinating for cyberspace support.⁴⁷

The services and joint force should revise Joint Unconventional Warfare doctrine in accordance with the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 5120.02B to identify the roles, responsibilities, and relationships among the joint force elements conducting and supporting Unconventional Warfare. In addition, the revised doctrine should provide guidance on the operational behavior of the Special Operations Forces conducting Unconventional Warfare across all domains to include Cyberspace and the physical, informational, and human factor-related dimensions of the information environment.⁴⁸

Organization. Organizational changes include the requirement for Special Operations Forces Service Components to recommend end-strength organizational structure to integrate Cyberspace support in operations. Changes recommended will likely come from within the USSOCOM enterprise at the cost of other existing programs, based on current budgetary constraints, although Special Operations Forces continue to realize future growth.

The design of new Cyberspace organizations is occurring across the force. The Army recently created units to provide service-specific enablers to the joint force. Following the creation of The United States Cyber Command in June 2009, the U.S.

Army activated the U.S. Army Cyber Command, 2nd Army in October 2010. The Army Cyber Command, plans, coordinates, integrates, synchronizes, directs, and conducts network operations and defense of all Army networks, and when directed, conducts Cyberspace operations in support of full spectrum operations in Cyberspace to ensure U.S./Allied freedom of action, and deny the same to adversaries.⁴⁹

The Army's activation of the 780th Military Intelligence Brigade as the Army's "first-of-its-kind" Cyber Brigade on December 1, 2011, provided a unit to counter an adversary operating in the highly technical, man-made domain of cyberspace.⁵⁰

USSOCOM and U.S. Army Special Operations Command (USASOC) should leverage the expertise within these organizations, and ensure Special Operations Forces requirements are integrated and synchronized.

Training. Training changes include the recommendation that USSOCOM should standardize training for Cyberspace operators across all the Special Operations Forces Service Components to achieve better efficiency and interoperability. USSOCOM should increase investment in training in Cyberspace capabilities, to include the requirement to develop and provide direction to components regarding minimum training standards for core skills required for Cyberspace support to Special Operations Forces. These skills include core Cyber operator skills required for special operations support, consensus on minimum courses and certifications that provide the core skills (include names, lengths, costs, proponent for each course or certification), any non-component unique combat skills training and courses that may run as joint courses, and gaps by component for training to meet specific mission profile in Cyberspace or combat.⁵¹

For Cyberspace training and skills for Network Operations, Network Defense, and Information Assurance, USSOCOM should establish enterprise core skills, minimum training standards, and required curriculum, including identification of core network operations skills required for support of Special Operations. USSOCOM should obtain consensus on minimum courses and/or certifications to provide required core skills, and identify by component any gaps each has regarding training, whether cyber or combat, to meet a specific mission profile. USSOCOM should review the Marine Corps Special Operations Command (MARSOC) and the Joint Special Operations Command (JSOC) training programs for applicability and expansion for all components, and identify a mechanism to track personnel trained; determine required training and certification required for operators and analysts to work within and leverage the national Signal Intelligence / Counter Network Exploitation platforms; and establish minimum entry standards for personnel ordered into those positions.⁵²

Materiel. Materiel change recommendations continue to stress defensive security of the computer network. Much effort is focused on the mitigation of Insider threats. USSOCOM should assign priority to provide funding for this capability, to include funding to support sustained capability. USSOCOM should continue to engage USCYBERCOM and ARCYBERCOM for materiel solutions, modified as necessary for use by Cyberspace personnel working with Special Operations Forces.

Leadership and Education. Within Leadership and Education, change recommendations include USSOCOM providing vision and guidance to Special Operations Forces Service Components. Currently, components' vision for employment of full-spectrum Cyberspace operations vary greatly within their tactical and operational

environments. Strategic-level staffs and leaders must understand Unconventional Warfare and its applications in Cyberspace to support Theater Campaign Plans and operations for Combatant Commanders. Education of senior strategic leaders is imperative. The U.S. Army War College released its 2011 edition of the Information Operations Primer, which includes new sections on U.S., DoD, and Army Cyberspace.

Personnel. For Personnel changes, USSOCOM must provide vision and guidance to Special Operations Forces Service Components on task organization of Cyberspace personnel to best leverage their expertise to conduct operations. USSOCOM should increase investment in Cyberspace personnel capabilities, and develop and provide direction to components regarding core skills required for support, including core Cyberspace operator skills required for Special Operations support.

Currently, the majority of the certified Cyberspace operators come from within the services. Services should train and certify Cyberspace operators to maintain proficiency and professional development throughout their careers. Special Operations Forces Service Components would screen and select Cyberspace operators to train for Special Operations Forces-specific requirements. USSOCOM should provide the training standards to service components and ensure compliance.⁵³

The Army must continue to project growth for Cyber units, and Military Occupational Specialty (MOS) “Cyber-Warriors.” The Army must anticipate turn-over and increase in demand to support other units as enablers, as the new Cyber unit incrementally fills its ranks. It is critical that the Army institutionalize the capabilities demanded of Cyberspace personnel in personnel systems, and joint / service manning documents. Recruiting the right personnel may require additional bonuses for

requirements in this technical and emerging field. Programmers must also capture the acquisition and sustainment of new Cyberspace equipment and future plans and budgets. Emerging programs of record may be required to provide sustainment of present and developing systems, as well as experimentation funds.⁵⁴

The total ARCYBER Command strength will exceed 21,000 Soldiers and civilians and the Army must fund it with existing fiscal resources.⁵⁵ The Army must continue to prioritize recruitment, development, and retention of Army Cyber experts.

ARCYBERCOM is prioritizing the following:

- Define Cyber personnel, training, and leader development requirements
- Define a Cyber Warrior Development Strategy (AC, RC, and DA Civilians)
- Create Cyber Programs of Instruction for Inclusion in all Individual Training
- Propose an Incentive Plan for HQDA to Recruit the required Cyber Work Force
- Propose an Incentive Plan for HQDA to Retain their Cyber Work Force
- Determine Knowledge, Skills, and Abilities Standards for Cyber Personnel⁵⁶

Facilities. Current facilities for training Unconventional Warfare reside at the the John F. Kennedy Special Warfare Center (JFKSWC) at Fort Bragg, NC. Cyber training must integrate into Unconventional Warfare training. Since services should continue to train Cyberspace personnel to support Special Operations Forces, most of the facility changes will be joint or service provided. With current budget constraints, USCYBERCOM should consider consolidation of Cyberspace training across the Department of Defense, with possible integration with other agencies' Cyberspace operators.

Policy. Policy changes are the most important to enable Special Operations Forces to conduct Unconventional Warfare within Cyberspace. Although U.S. Strategic Command and U.S. Cyber Command are Department of Defense proponents for the Cyber domain, it is imperative that the Special Operations community, as well as the services and other agencies identify areas that require their specific expertise, capabilities, and authorities in coordination with U.S. Cyber Command. Current U.S. and Department of Defense policies and authorities for Cyberspace operations limit Special Operations Forces' ability to execute full-spectrum operations. In order to effectively utilize the Cyberspace Domain for Special Operations, Special Operations Forces will require their own set of authorities to conduct the full range of activities in and through Cyberspace to support missions. USSOCOM should establish a Cyber Capabilities Product Line within USSOCOM's acquisition directorate, Special Operations Research, Development and Acquisition Center (SORDAC) under the appropriate Program of Record; create a Capability Development Document (CDD) for Special Operations Forces' Cyberspace capabilities; and assign a formal Cyber lead in SORDAC's Science and Technology Division.⁵⁷

Many Americans remain ambivalent about covert operations; however, current law provides for the use of covert operations as a tool for national security. The Unconventional Warfare legislation represents a balance between the requirements of secrecy versus accountability, and agility versus deliberation. Laws, regulations, and executive orders may need revision to meet current threats, especially in Cyberspace. It is imperative that a consensus is reached about what measures are legal and effective. The recent emergence of an Unconventional Warfare threat in Cyberspace

offers opportunities to resolve fundamental national security issues and produce a new, comprehensive charter for Special Operations Forces to operate in Unconventional Warfare and other missions.⁵⁸

Conclusion

Potential adversaries of the United States have conducted, and will continue to conduct Unconventional Warfare within Cyberspace within the United States and abroad. The success of al Qaeda in recruiting members from within the United States via the internet to train, plan, and execute terrorist plots is one example of its effectiveness. The Joint Force must not overlook the need to bolster the Special Operations Forces' ability to conduct Unconventional Warfare, but most importantly, how to do it within the new Cyberspace Domain.

The Special Operations community is placing a heavy emphasis on Unconventional Warfare as a core mission, and continue to look critically at the capability gaps and potential solutions to ensure the necessary skill sets are inherent in operators for the future. With the newly defined domain of Cyberspace receiving priority as an evolving critical variable in the operating environment, it is critical that Special Operations Forces define and establish roles and responsibilities within Cyberspace to enable all phases of Unconventional Warfare.

USSOCOM must continue to emphasize the training of U.S. Special Forces in the conduct of Unconventional Warfare in a Cyberspace Domain, ensuring personnel from the Services are fully prepared. It should continue to work with the administration and other agencies to support the use of Special Operations Forces in Cyberspace, to ensure that the necessary authorities, policies, and the will to use Unconventional Warfare as a means to operate in Cyberspace to take offensive measures, rather than

only reacting to Cyber threats. It must synchronize efforts with U.S. Cyber Command, and U.S. Army Cyber Command, to ensure the necessary Unconventional Warfare tactics, techniques, and procedures as they pertain to the Cyberspace domain are specified within concepts, doctrine, and operational procedures to provide the necessary authorities, roles, and missions that are peculiar to Special Operations. The impending risk of not pursuing the recommended DOTMLPF-P recommended solutions is allowing potential adversaries to advance to parity or supremacy over the United States' current Cyberspace capabilities, leaving forces and the nation vulnerable.

Endnotes

¹ Martin E. Dempsey, *Chairman's Strategic Direction to the Joint Force* (Washington, DC: U.S. Department of Defense, February 2012), 6.

² Maria Camila Pérez, "Facebook Brings Protest to Columbia," *New York Times Online*, February 8, 2008, http://www.nytimes.com/2008/02/08/business/worldbusiness/08iht-protest11.html?_r=1 (accessed March 15, 2012).

³ Linda Robinson, *Masters of Chaos: The Secret History of the Special Forces*, (Public Affairs, Perseus Books Group, New York, 2004), xvi.

⁴ Catherine Herridge, *The Next Wave, On the Hunt for Al Qaeda's American Recruits*, (New York: Crown Publishing Group, Random House, Inc., 2011), 21.

⁵ *Ibid.*, 32.

⁶ U.S. Joint Chiefs of Staff, *Unconventional Warfare Joint Integrating Concept*, (Washington DC: U.S. Joint Chiefs of Staff, February 2, 2010).

⁷ United States Special Operations Command, *Special Operations In and Through the Cyberspace Domain (SOCD) version 0.4*, White Paper Draft, (MacDill Air Force Base, FL: 31 January 2012).

⁸ *Ibid.* U.S. Joint Chiefs of Staff, *Unconventional Warfare Joint Integrating Concept*.

⁹ U.S. Joint Chiefs of Staff, *Department of Defense Strategy for Operating in Cyberspace*, (Washington DC: U.S. Joint Chiefs of Staff, July 2011).

¹⁰ *Ibid.*

¹¹ Leon E. Panetta, *Defense Strategic Guidance* (Washington DC: Office of the Secretary of Defense, January 2012).

¹² Ibid.

¹³ Ibid.

¹⁴ Ibid.

¹⁵ Ibid.

¹⁶ Ibid.

¹⁷ Ibid.

¹⁸ John H. McHue, Secretary of the Army, "Enclosure 1 to Fragmentary Order 64 to TCP 11-12 Secretary of the Army Top Priorities," Department of the Army, Washington DC, February 2012.

¹⁹ Anthony Bullard, *Conducting Unconventional Warfare Using the Internet, United States Special Operations Command White Paper version 1.0*, (MacDill Air Force Base, FL, April 28, 2010).

²⁰ Ibid. Panetta.

²¹ Ibid.

²² U.S. Army Cyberspace Home Page, <http://www.arcyber.army.mil/> (accessed March 15, 2012).

²³ Huba Wass de Czege, *Warfare by Internet: The Logic of Strategic Deterrence, Defense, and Attack* *Military Review Online*, Volume XC — July–August 2010, No. 489 Headquarters, Department of the Army, U.S. Army Combined Arms Center, Fort Leavenworth, Kansas, , <http://militaryreview.army.mil>, Professional Bulletin 100-10-7/8 (accessed March 15, 2012).

²⁴ Ibid. Dempsey, 4-6.

²⁵ Ibid. 8.

²⁶ William H. McRaven, *United States Special Operations Command Posture Statement*, Posture Statement presented to the 112th Congress Armed Services Committee (Washington DC: March 6, 2012), http://www.fas.org/irp/congress/2012_hr/030612mcraven.pdf (accessed March 15, 2012).

²⁷ Ibid. Bullard.

²⁸ Hina Samnani and Lolla Mohammed Nur, "Crowdmapping Arab Spring - Next Social Media Breakthrough?" June 28, 2011, <http://www.voanews.com/english/news/middle-east/Crowdmapping-Arab-Spring-Next-Social-Media-Breakthrough--124662649.html> (accessed March 15, 2012).

²⁹ Ibid. Bullard.

³⁰ Ibid.

³¹ Ibid. Herridge, 19.

³² Ibid. 41.

³³ Ibid. Bullard.

³⁴ Camille C. Chidiac, Michael Stone, and Michael Wilde of Wpromote, Incorporated, briefing to Colonel Denton Knapp, U.S. Army, Director J7/9-F, U.S. Special Operations Command, June 2011.

³⁵ Ibid.

³⁶ Ibid.

³⁷ Ibid. Bullard

³⁸ Ibid.

³⁹ Ibid.

⁴⁰ Ibid.

⁴¹ Ibid.

⁴² Leon E. Panetta, *Defense Budget Request, Written Submitted Statement to the Senate Armed Services Committee*, 112 Congress, February 14, 2012.

⁴³ Henry Kenyon, "DARPA to Develop Offensive Cyberspace Capabilities: Researchers Focus On Offensive and Defensive Cyber Tools," November 7, 2011, <http://defensesystems.com/articles/2011/11/07/darpa-offensive-cyber-capabilities.aspx> (accessed March 15, 2012).

⁴⁴ Ibid.

⁴⁵ Ibid. Bullard

⁴⁶ Ibid.

⁴⁷ Ibid.

⁴⁸ Ibid.

⁴⁹ U.S. Army Cyber Command webpage <http://www.arcyber.army.mil/org-arcyber.html> (accessed March 15, 2012).

⁵⁰ Tina Miles, 780th Military Intelligence Brigade, "Army activates first-of-its-kind Cyber Brigade, December 9, 2011, <http://www.army.mil/article/70611/Army> (accessed March 15, 2012).

⁵¹ Ibid. Bullard

⁵² Ibid.

⁵³ Ibid.

⁵⁴ Ibid.

⁵⁵ Ibid. U.S. Army Cyberspace Home Page.

⁵⁶ Ibid.

⁵⁷ Ibid. Bullard.

⁵⁸ Ibid. Robinson, 368.

