Strategy Research Project

LEVERAGING CYBERSPACE IN COUNTERINSURGENCY OPERATIONS

BY

COLONEL AARON A. WEBSTER
United States Army

USAWC CLASS OF 2010

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State 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

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
08-02-2010	Strategy Research Project	

4. TITLE AND SUBTITLE

Leveraging Cyberspace in Counterinsurgency Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel Aaron A. Webster

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Dr. Jeffrey L. Groh
Department of Distance Education

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: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Military forces today are facing traditional, irregular, catastrophic, and disruptive challenges. U.S. military forces are conducting counterinsurgency operations (COIN) in populated neighborhoods amongst innocent people. The enemy is using insurgency and hybrid warfare to make it more difficult for the United States and coalition forces to employ kinetic weapon systems and technology. This paper argues that the use of cyberspace by insurgents is more prominent, lethal, and difficult to defeat. The paper will use operations in Afghanistan as a case study.

First, this paper will provide background of how forces predominantly fought in the past and employed conventional weapons in Counterinsurgency operations. Second, the author will clearly define cyberspace and present an in-depth discussion into the employment techniques, challenges and advantages of this readily available technology. Next, the paper will discuss Computer Network Attack (CNA), Computer Network Defense (CND), agencies and in theater policies at the strategic level. Lastly, the paper will close with a few recommendations that provide techniques to safeguard theater networks, resources and means to limit the numerous cyber challenges.

15. SUBJECT TERMS

Computer, Network, Internet, Security, Hacking, Virus, Attack, Defense, Cyber, Insurgent

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	30	

USAWC STRATEGY RESEARCH PROJECT

LEVERAGING CYBERSPACE IN COUNTERINSURGENCY OPERATIONS

by

Colonel Aaron A. Webster
United States Army

Dr. Jeffrey L. Groh
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.

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

ABSTRACT

AUTHOR: Colonel Aaron A. Webster

TITLE: Leveraging Cyberspace in Counterinsurgency Operations

FORMAT: Strategy Research Project

DATE: 8 February 2010 WORD COUNT: 5,752 PAGES: 30

KEY TERMS: Computer, Network, Internet, Security, Hacking, Virus, Attack, Defense, Cyber, Insurgent

CLASSIFICATION: Unclassified

Military forces today are facing traditional, irregular, catastrophic, and disruptive challenges. U.S. military forces are conducting counterinsurgency operations (COIN) in populated neighborhoods amongst innocent people. The enemy is using insurgency and hybrid warfare to make it more difficult for the United States and coalition forces to employ kinetic weapon systems and technology. This paper argues that the use of cyberspace by insurgents is more prominent, lethal, and difficult to defeat. The paper will use operations in Afghanistan as a case study.

First, this paper will provide background of how forces predominantly fought in the past and employed conventional weapons in Counterinsurgency operations. Second, the author will clearly define cyberspace and present an in-depth discussion into the employment techniques, challenges and advantages of this readily available technology. Next, the paper will discuss Computer Network Attack (CNA), Computer Network Defense (CND), agencies and in theater policies at the strategic level. Lastly, the paper will close with a few recommendations that provide techniques to safeguard theater networks, resources and means to limit the numerous cyber challenges.

LEVERAGING CYBERSPACE IN COUNTERINSURGENCY OPERATIONS

Insurgents in Afghanistan interpret and use cyber-generated information and actions differently than U.S. operators. This is because the insurgents' context for decision making (no need to adhere to any law other than their own interpretation of the Koran), jihadist prism for viewing the environment, and indifference to killing innocent people allows them to intimidate, influence and mobilize their believers in ways unacceptable to civilized commanders.[1] The enemy is using insurgency and hybrid warfare to make it more difficult for the United States and Allied forces to employ kinetic weapon systems and technology. This paper argues that the use of cyberspace by insurgents is more prominent, lethal, and difficult to defeat in coalition operations in Afghanistan

First, this paper will provide background of how forces predominantly fought in the past and employed conventional weapons in Counterinsurgency operations. Second, the author will clearly define cyberspace and present an in-depth discussion into the employment techniques, challenges and advantages of this readily available technology. Next, the paper will discuss Computer Network Attack (CNA), Computer Network Defense (CND), agencies and in theater policies at the strategic level. Lastly, the paper will close with a few recommendations that provide techniques to safeguard theater networks, resources and means to limit the numerous cyber challenges.

Counterinsurgency Operations

During the initial phases of Operation Iraqi Freedom (OIF), just 43 days after announcing the start of the war in Iraq, President George W. Bush on Thursday tells the nation that "major combat operations in Iraq have ended."[2] In Operation Desert Storm,

the U.S.-led coalition bombarded Iraqi targets with airstrikes for 38 days, softening Iraq for a ground offensive that lasts only 100 hours before Iraq retreats from Kuwait and negotiates an end to the war.[3] In each battle the enemy is easily identifiable and in a position to use their country's conventional weapon systems in defense of their objectives, positions and beliefs. Coalition forces superior firepower and airspace dominance easily allows the destruction of the enemy's command and control and key weapon systems breaking their will to continue to fight.

This is not the case in Afghanistan. Coalition forces are fighting against insurgents who blend in with the local populace and hide in mountain caves. These insurgents are not using conventional weapons and fighting force on force but use improvised explosive devices (IEDs), suicide bombers and more importantly cyberspace. The use of cyberspace by terrorists and insurgents is the tip of a technology iceberg that's changing the nature and lethality of the threat they pose.[4] Because cyberspace is critical to the enemy's success, coalition forces must be aware of the tactics and methods and creatively implement effective cyber counter techniques in the counterinsurgency operations plans.

The Department of Defense (DoD) acknowledges that cyber/information warfare through media and other technology is the key to winning on the battlefield. Dating back to Sun Tzu's teachings, information warfare is the offensive and defensive use of information and information systems to deny, exploit, corrupt, or destroy an adversary's knowledge, communications, and perceptive access and processes.[5] Cyberspace achieves costless advantages over one's adversaries and can be a supplement or a replacement for traditional military operations.[6]

U.S. military personnel are shifting from their basic occupational specialty and retrain to hone infantry warrior and civil affairs skills in support of counterinsurgency. For example, because of the limited use of the Navy's resources, many of the sailors train as ground forces and provide other specialty services such as medical, construction, and trainers for the local population. In January 2009, Adm. Gary Roughead, the Chief of Naval Operations visits Sailors working with the Provincial Reconstruction Team in Afghanistan. During his visit he stated that "working in one of the most kinetic province of Afghanistan, you have completed a laundry list of projects, from helping to establish an adequate healthcare system to standing up a landmark program known as the Konar Construction Centre. You graduate approximately 150 students (locals) every month in electrical work, plumbing, and general construction. When you get back into a normal Navy assignment, the way you think and how you're going to be able to do more things is going to make you stand out."[7] As military members train to focus on counterinsurgency, they must also be aware of the enemy's effective use of cyberspace.

Emphasis on Minimal to no Collateral Damage

General McChrystal's guidance does not necessarily focus on killing insurgents. The guidance states that coalition forces will help the Afghan people win by securing them, protecting them from intimidation, violence, abuse and by operating in a way that respects their culture and religion. "This means coalition forces must change the way they think, act, and operate. Large scale operations to kill or capture militants carry a significant risk of causing civilian casualties and collateral damage. If civilians die in a firefight, it does not matter who shot them – we (coalition forces) still failed to protect them from harm. Destroying a home or property jeopardizes the livelihood of an entire

family – and creates more insurgents".[8] Cyberspace is a valuable resource when ensuring media and communication assets broadcast coalition successes and intent.

Cyberspace in Counterinsurgency

Counterinsurgency operations entail a vastness of data and information that is shared by not only coalition forces but government agencies up to the President of the United States. Cyberspace considerably strengthens the ability and capability of all actors to influence the battlefield. Coalition forces in Afghanistan face known and unknown challenges to protect and defend its cyber resources while at the same time using cyberspace favorably to accomplish their mission. Cyberspace resources include the Internet, telephone system, and other devices in the virtual environment. Insurgents diligently use cyberspace to achieve objectives and effects as well as a recruiting tool for prospects with the same beliefs. Due to the speed at which cyber technologies change and improve, the cost and availability of commercial-off-the- shelf cyber tools is inexpensive and easy to acquire. Coalition forces must remain ahead of the fast pace advances in technology and leverage cyberspace to understand what the insurgents intend to do, their objectives, and to counter their propaganda to the populace.

Cyberspace Definition

The Department of Defense "dictionary", Joint Publication 1-02, had a definition of cyberspace dating to the early 2000s, but there was virtually universal agreement that it was insufficient: "the notional environment in which digitized information is communicated over computer networks."[9] Cyberspace is hardly "notional", and confining it to "digitized and computerized" is far too limiting, failing to reflect the massive technological and social changes with which cyberspace is interwoven.[10] Since the mid-1990s several authors, to name a few, (Greg Rattray, *Strategic Warfare*

in Cyberspace (2001), Dorothy Denning, *Information Warfare and Security* (1999), Walter Gary Sharp, *CyberSpace and the Use of Force* (1999), and Winn Schwartau**,** *Information Warfare: Chaos on the Electronic Superhighway* (1994)) offered useful insights and perspectives that helps shape thought on this issue, and the proposed definition.[11] Several consistent threads run through these references, including the role of telecommunications infrastructures, electronics, and information systems.[12]

A crucial perspective, offered by the White House's 2003 "National Strategy to Secure Cyberspace", which defines cyberspace as the "nervous system—the control system of the country….composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allows our critical infrastructures to work."[13] The Joint Staff in early 2006 initiated an important and needed effort to develop a "National Military Strategy for Cyberspace Operations". The Chairman of the Joint Chiefs of Staff, General Peter Pace, in mid-December 2006, it states that "Cyberspace is a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked information systems and physical infrastructures."[14] As stated countless definitions may exist but a May 12, 2008 "for official use only" memo signed by Deputy Defense Secretary Gordon England, titled "the definition of cyberspace," offers a 28-word meaning for the term.[15] Cyberspace, England writes, is "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."[16] The Internet serves as

an intelligence and reconnaissance asset for Jihadist even in the planning stages of armed conflict.[17]

Insurgents Use of Cyberspace

Insurgents in Afghanistan can posses information superiority and the information advantage because their physical location and identity can remain hidden behind websites and fake email accounts. Since 9/11 the growth of extremist related Web sites has grown significantly to well over 4,500. Many of these sites strongly advocate Al Qaeda's ideology and involves into virtual bases for recruiting, training, coordinating attacks, sharing information, fund raising (even using Pay Pal) and influence. The Taliban and Al Qaeda in Afghanistan use the Internet for cyber-mobilization allowing many of their followers and other extremist groups to come together quickly in chat rooms to plan and coordinated activities.[18]

Common cyberspace stealth methods used by insurgents include encryption, domain name changing, fuse of proxy servers to obscure locations, and "dead dropping," where information remains as draft messages in fake email accounts.[19] These email accounts are accessible to anyone with a password, thereby avoiding transmission and detection.[20] Considering the hundreds of thousands of servers and Internet Service Providers (ISPs) worldwide, plus the billions of bytes passing over the network every second, the insurgent has a large playing field to roam.[21]

In Afghanistan, the Taliban banned television and even toothbrushes as forbidden modern innovations. Yet al Qaeda, led by educated and privileged gadget hounds, adapted early and enthusiastically to the technologies of globalization, and its Arab volunteers managed to evade the Taliban's screen-smashing technology police. [...] bin Laden and his deputy, Ayman Zawahiri, have fallen well behind their younger

followers worldwide. The two still make speeches in a makeshift studio and courier their message at considerable risk to Al-Jazeera or other satellite stations, as with Zawahiri's messages. Their younger adherents have moved on to Web sites and the production of short videos with shock appeal that is broadcast to millions instantly via the Internet.[22]

Insurgents throughout Afghanistan are creative and use deceptive techniques such as “hide in plain site”. This technique involves, what appears to be, a standard website of everyday advertisement such as Arab entertainment. To the common internet surfer this means nothing but to the trained eye or potential insurgent the site posses a trigger link, only visible for a short time, which will take the surfer to an extremist insurgent website. This is cyber deception whereas the access point cyber-vanishes in a short period of time. Techniques such as “hide in plain site” and cyber deception are not easily found nor is the site traceable to a single location, computer, or individual before the insurgent realizes the compromise and makes a change. [23]

In some cases insurgents use IEDs to distract, disrupt, or delay opposing forces facilitating another attack. Insurgents do not detonate these destructive devices manually but through the use of cell phones; another cyber tool. A radio-controlled IED incorporates a modified cell phone with an electrical firing circuit. Cell phones operate in the Ultra High Frequency (UHF) band in line of sight with base transceiver station (BTS) antennae sites. Commonly, receipt of a paging signal by phone is sufficient to initiate the IED firing circuit.[24] All of the tools and resources used to design, build and detonate these destructive devices are easily accessible and clearly an indicator that insurgents are becoming more and more cyber savvy.

Acquisition of Cyber Resources

Coalition forces in Afghanistan periodically find cyber tools used by insurgents. Intelligence confirms that the cyber tools are for communicating with other insurgents for potential IED emplacement locations. This is clearly evidence that insurgents have the means to fund and acquire cyber resources at will. Through the availability of the Internet, insurgents no longer have to travel throughout the country or even to a local medium to purchase their equipment. Sites such as Ebay, Amazon, and countless U.S. retailers will unknowingly or knowingly ship cyber resources to insurgents once they pay for the items. Insurgents are constantly moving from place to place, between Afghanistan and Pakistan, and are difficult to trace. Today, cyber tools sold around the world continue to be a click away for insurgents to purchase. Insurgents in Afghanistan attempt to broadcast their message for attacks and bombings to other cells so that they can destroy or kill as many innocent people as possible.

Methods to Coordinate and Advertise Insurgent Propaganda

The Virtual Afghanistan is the network of hundreds of Jihadist Web sites that inspire, train, educate and recruit young Muslims to engage in jihad against America and the West.[25] In December 2005, the Middle East Media Research Institute reports that insurgents are using Yahoo.com as a gateway for indoctrination and incitement of aspiring insurgents.[26] An al Qaeda video library found on the Web and obtained by *The Washington Post* from a researcher with experience shows in a series of high-quality training films shot in Afghanistan on how to conduct a roadside assassination, raid a house, shoot a rocket-propelled grenade, blow up a car, attack a village, destroy a bridge and fire an SA-7 surface-to-air missile.[27]

Notably, Taliban information campaigns revolve around perceptions and sentiments of those affected by Coalition actions.[28] Not only are the Taliban campaigns more thorough, they also incorporate aspects of honor, history, and tradition to summon the support of the people.[29] Insurgents are extremely aggressive with getting their message out through the use of the Internet, media, websites, radio, chat rooms, and other cyber tools. With the Soviet invasion not far from the memories of Afghan people, they compare the atrocities of this conflict to the indiscriminate actions of the previous war, drawing parallels to undermine Coalition efforts.[30]

Nonetheless, it is the Coalition who finds itself in a defensive stance, not only to counter the Taliban propaganda but to gain legitimacy from a populace that is losing confidence in its efforts.[31] In the end, it is the Afghan people who will determine victory or defeat; Taliban seem to know this fact while the “liberators” often appear to overlook the power of such information.[32] So successful have the militants become at propaganda that many analysts doubt that the group achieved the transformation alone. Joanna Nathan, an Afghan analyst who writes extensively on Taliban propaganda, blames “outside assistance from the media-savvy al-Qaeda”.[33] “The Taliban blow stuff up to create an event that they can then market to the media and that will shape public perceptions,” Rear Admiral Greg Smith, the foremost communications expert in the U.S. Navy, says.[34] “The Taliban have embedded communications at the very heart of their operations, with terror attacks and assassinations having a psychological impact far beyond the immediate victims both in Afghanistan and around the world,” Ms Nathan says.[35] “That is the nature of insurgency — not winning battles, but seeking to portray

omnipresence and a determination to stay the course."[36] These new cyber techniques present new and difficult challenges to Coalition forces.

Friendly Forces Cyber Challenges

Fighting and defeating insurgents in Afghanistan by using cyberspace for Counterinsurgency operations is one of the leading concerns not only for the CENTCOM Commander, General David Petraeus., but the lead commander in Afghanistan, General Stanley McChrystal. The Taliban and Al Qaeda are the first guerrilla movement in history to migrate from physical space to cyberspace.[37] Using laptops and DVDs, in secret hideouts and at neighborhood Internet cafes, young code-writing jihadists have sought to replicate the training, communication, planning and preaching facilities they lost in Afghanistan with countless new locations on the Internet.[38]

U.S. Joint and Army Information Operations doctrine maintains that achieving information superiority (IS) is a critical factor for success in military operations. Yet, for the past four years, U.S. forces are unable to achieve true IS in Afghanistan. While possessing an overwhelming edge in information technology to achieve IS, U.S. forces are faltering in one critical area: denying the enemy the ability to collect, process and disseminate an uninterrupted flow of information.[39]

Western nations lose credibility when NATO denies high civilian death tolls that are subsequently proven correct. Last year, NATO ridiculed claims that up to 90 civilians had died in a U.S.-led operation in Farah province, admitting to a toll of five dead. The U.S. began to backtrack after *The Times* and other media obtains mobile phone footage of dozens of dead men, women and children. Rear-Admiral Smith acknowledges that NATO is often flatfoot and their television advertisements and

newspapers are only “marginally effective” in a largely illiterate society with little electricity.[40]

Coalition forces in Afghanistan face tremendous cyber challenges because cyberspace, one of the preferred weapon systems of the enemy, is extremely hard to locate, identify and capture. In Afghanistan, General Petraeus and General McChrystal are trying to imitate the highly effective command structure established in Iraq, “one truly optimized over time for the conduct of counterinsurgency operations.” General Petraeus said a host of essential “enablers” are still on the way to Afghanistan, a reference to either national level intelligence operators and special operations forces or more surveillance drones and aircraft, or both. General Petraeus dispels any notions that cyberspace operations might not be the threat some make it out to be. He identifies U.S. capabilities in cyberspace as one of the “big capabilities” that is lacking, and one he highlights to the Quadrennial Defense Review (QDR) strategic review team. “Cyberspace is a battleground, it cannot be uncontested, and the enemy cannot have free reign out in cyberspace anymore than they have free reign in a geographical location.”[41]

Cyber Method to Counter Insurgent Propaganda and Cyber Tactics

Information operations are a critical aspect of warfare and will help determine the outcome in Afghanistan, focusing on the trust and confidence of the Afghan population.[42] Thomas Friedman states, “What is really scary is that this violent, jihadist minority seems to enjoy the most ‘legitimacy’ in the Muslim world today.[43] Few political and religious leaders dare to speak out against them in public.” While it’s true that jihadists are a minority, they are certainly not held in high esteem, as Mr. Friedman suggests. For instance, a leading Pakistani cleric, Sarfraz Ahmed Naeemi, was killed by

a suicide bomber because he is a critic of the violence the Taliban is committing. Not alone, he is the driving spirit of a group of over 20 religious parties raising their voices against the violence of the by the Taliban.[44]

General McChrystal states in his Commander's Initial Assessment to the Secretary of Defense that "we cannot focus our strategy on seizing terrain or destroying insurgent forces; our objective must be the population."[45] HQ International Security Assistance Force (ISAF) must understand and adapt to the immediacy of the contemporary information environment through the employment of new/ social media as well as cell phones, TV, and radio to promote interactive communication between Afghan and international audiences.[46] This will involve a significant investment in technical architecture.[47]

Al Qaeda, Taliban and other insurgents, through websites and radio broadcasts, threaten the Afghan people by telling them that they must not violate Sharia law. Immediately after any skirmish or airstrike, if there are civilian casualties, the Taliban or al Qaeda broadcast that American forces kill innocent civilians including women and children. These Insurgents are always first on the cyber airwaves with any form of announcement broadcasting their version of what took place. American and Coalition forces are continuously several hours to several days behind the insurgents initial broadcast in attempting to portray the true story of what took place. By the time a coalition broadcast is made, the Afghan populace is already irate and angry at what they perceive as American negligence and mistakes. To defeat this negative propaganda, the coalition commanders and media must aggressively use all cyber means available to get the correct message out to the populace first. It does not matter

if the death of an innocent child is caused by an air strike, suicide bomber, or IED, the coalition should flood the cyber airwaves with pro-Afghan messages telling the populace how the U.S. lead forces are not killing innocent people. General McChrystal states that "new procedures must be developed for sharing information about such events so that when they happen, we are first with the truth."[48]

General McChrystal recommends expansion of the Afghan strategic communications program following public calls for such a step by the chairman of the Joint Chiefs of Staff, Adm. Mike Mullen, and by Richard C. Holbrooke, the U.S. special envoy to the region.[49] Holbrooke complains that the Taliban communicates more effectively than the United States. Holbrooke also told a House subcommittee in June that there is a need to refine the coalition's message and use new ways to reach Afghans, suggesting cell phones, radio and other means.[50] NATO's new communications directorate opened in Kabul this year and employs a 120 person staff.[51] "Information is everything.[52] This is a war of perception played out in the minds of the Afghan people," says Admiral Smith. His arrival in Kabul in May is the latest acknowledgement that in the front rooms of the West and the villages of Afghanistan, NATO fails to win the argument.[53]

Countering and Collecting Insurgent Media

Although insurgents have camps and hideouts in caves and mountainous areas, the most elusive location where they perform the most damage is the Internet. Through the use of the Internet, Taliban and other extremist organizations have numerous websites such as www.alneda.com and www.hazara.net/taliban/taliban.html, which are currently shutdown. However, they consistently devise methods to develop, populate and advertise new ones. Insurgents continue to marshal the media to "destroy armies"

since they began their armed campaign in 2003.[54] Their media campaign uses the Internet to target educated, influential segments of the Arab population, and they can reach an audience of millions when the mainstream media pick up their diatribes or news bulletins.[55] Unencumbered by a centralized bureaucracy or a brick-and-mortar infrastructure, the Sunni insurgent media network is efficient and fast-moving.

The CENTCOM Commander directs that his J6, Public Affairs Officer and other staff principles become aggressive with not only gathering valuable data from enemy websites but getting with the appropriate agencies to shut down the ones contrary to U.S. interests. In Afghanistan, troops train to gather any media or cyber tools left behind by insurgents when clearing hiding areas. This media, in some cases, can determine intent and possible techniques the enemy may use in future attacks on the military or the populace. The more cyber utensils and weapons the Coalition can take out of enemy hands, the better chance of winning in cyberspace. However, this task is not easy because cyberspace is freely available to anyone who has the propensity to purchase it.

NATO is only now in the process of catching up, aware that it faces an uphill battle. In August, U.S. Special Envoy Richard Holbrooke establishes a new unit within the State Department for countering militant propaganda in Afghanistan and Pakistan – in other words engaging in strategic communication. According to *The New York Times*, the Holbrooke effort has funds to the tune of $150 million. Holbrooke told Tom Shanker of *The New York Times*, “Concurrent with the insurgency is an information war. We are losing that war. The Taliban have unrestricted access to radio, which is the main means of communication. We can’t succeed, however you define success, if we cede to people

who present themselves as false messengers of a prophet, which is what they do. We need to combat it."[56]

There are effective applications available that aid in basic intelligence gathering. Google Earth and similar programs are free and provide street-view photos of potential targets, as well as excellent route and obstacle information. The tendency of most Western countries to post nearly everything there is to know about critical infrastructures on unsecured Web sites is a great boon to the terrorists and requires no more expertise than an ability to use rudimentary search engines that small children master. All of this "research capability" assists the terrorists in making their standard operation procedures much easier and safer to polish to a high degree. Vigilance in protecting infiltration by cyber-insurgents must be on the front burner of all personnel to be successful.

Cyber Attack and Defense

There are millions of attempts on a daily basis to attack the cyber networks of the U.S. and Coalition systems supporting the ongoing counterinsurgency operation in Afghanistan. The attacks are attempts to gather intelligence, degrade, or destroy critical cyber systems to limit or disrupt the Commanders ability to command and control his forces. If the attacks are successful they may also limit the Commanders ability to communicate with the Afghan leaders and people.

Defending such attacks is extremely challenging not only for forces in Afghanistan but U.S. forces in the United States. The demand for protecting these critical systems is one that requires significant training, resources and support from agencies of all countries around the world. Cyber defense is a must if Coalition forces are to deny infiltration into military networks supporting the Afghan mission.

Computer Network Attack (CNA)

The Department of Defense (DoD) defines Computer Network Attack as - operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.[57] Like other Information Operations, CNA has implications across the warfare spectrum, the tactical, operational, and strategic levels of war. In Afghanistan, Computer Network Attacks provide many benefits over the conventional physical reduction of an enemy capability, or by the use of CNA at the tactical level to achieve these goals.

Cyber Vulnerabilities

Coalition Networks in Afghanistan are vulnerable to attack or compromise via viruses, Trojans or other means of commercial-off-the-shelf software. This tactic is evident by the recent acknowledgement by the Department of Defense that Insurgents in Iraq gained access to surveillance video from U.S. Drones flying the area. Using a $26 off-the-shelf software program, SkyGrabber, to intercept live video feeds from U.S. Predator drones, Insurgents have all they need to potentially monitor U.S. military operations.[58] SkyGrabber is an offline satellite internet downloader that intercepts satellite data (movie, music, pictures) downloaded by other users and saves the information in your hard disk.[59] Senior defense and intelligence officials said Iranian-backed insurgents intercepted the video feeds by taking advantage of an unsecure communications links in some of the remotely flown planes' systems.[60]

U.S. officials say there is no evidence that militants are able to take control of the drones or otherwise interfere with their flights. However, the intercepts could give the Taliban battlefield advantages by removing the element of surprise from certain missions making it easier for insurgents to determine which roads and buildings are

under U.S. surveillance. U.S. military personnel discovered the problem late last year when they apprehended a Shiite militant whose laptop contained files of intercepted drone video feeds. In July, the U.S. military found drone video feeds on other militant laptops, leading some officials to conclude that militant groups trained and funded by Iran were regularly intercepting feeds.

The drone intercepts mark the emergence of a shadow cyber war within the U.S.-led conflicts overseas. They also point to a potentially serious vulnerability in Washington's growing network of unmanned drones, which is the American weapon of choice in both Afghanistan and Pakistan. The stolen video feeds also indicate that U.S. adversaries continue to find simple ways of counteracting sophisticated American military cyber technologies.[61]

Computer Network Defense (CND)

The Department of Defense defines Computer Network Defense as actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DoD information systems and computer networks.[62] Prior to General McChrystal's appointment as the Commander in Afghanistan, his predecessor, General McKiernan, faced infiltration of his computer networks as the attackers used the agent.btz.

The agent.btz malware, a computer program that independently replicates by copying itself to other systems, is getting to other computer systems via flash drives. Defense officials did not describe the extent of damage on military networks but states the attack struck hard at networks within U.S. Central Command, the headquarters that oversees U.S. involvement in Iraq and Afghanistan, and affects computers in combat zones.[63] The attack also penetrated at least one highly protected classified network.[64] In response to the attack, the U.S. Strategic Command, which oversees the military's

cyberspace defenses, has raised the security level for its so-called information operations condition, or "INFOCON," initiating tighter security measures on military networks.[65]

The immediate ban of external drives produces an immediate negative impact on operations in Afghanistan as this is how the majority of information sharing takes place. General McKiernan confronted this dilemma with the CENTCOM Commander and requests that his Communications Directorate be the only agency given authority to purchase external media for the organization. With the initial verbal approval of CENTCOM, forces in Afghanistan could use external media from the Communications Directorate. This also involves a tremendous security campaign in theater to educate all forces on the seriousness of this attack and what they must do to continue to protect military networks and data.

CENTCOM took additional security measures by installing Thin Client systems on their networks. Thin Client computing works like a modern-day version of mainframe computing that use dumb terminals and central servers for data storage.[66] The end user sees no difference as all applications look and functions the same as if on a standard desktop. Data from different workstations or different locations is input into a central database. There are no hard drives or floppy drives only allowing data storage to the server. In fact, keystrokes, mouse events and screen images are all that is sent between the client and server. This makes the device much more secure than a standard desktop or notebook computer. Administrators' control all functions from back end servers which allow the command to lock all USB ports with the exception of those few that require access for mission essential tasks. Thin Client provides the command

more control over its networks and the updating of security patches to maintain protection. Thin Clients are currently functioning at the forward headquarters in Qatar and also being proliferated throughout Afghanistan. If a Thin Client is stolen by insurgents in Afghanistan, there is no compromise of data. This type of aggression and effort by CENTCOM and the ISAF Commander allows them to stay ahead of insurgents and other enemy attempting to defeat and infiltrate DoD networks in Afghanistan and at the Combatant Command Headquarters.

Recommendations

First, Central Command must continue to ensure the ISAF leadership in Afghanistan is aware of any network vulnerabilities found by Information Assurance (IA) personnel. Network security personnel in Afghanistan should constantly scan for viruses, worms, Trojans and any potential infiltration by unknown attackers. IA personnel should daily collect and scan the certified external media for the same vulnerabilities. The disadvantage to continuous network scans is the network in Afghanistan may become slightly slower causing a slight delay in mail deliverance or network speed. The potential risk to this recommendation is if IA does not perform the scans, immediate infection is inevitable as shown through past infiltrations. General McChrystal must feel comfortable that the data he and his staff are transmitting around the battlefield is secure and free of damaging viruses.

Second, coalition forces in Afghanistan must be first with publishing the known truth about all military actions potentially affecting or killing Afghan people. With the cyber technology available to the commander, the communication staff and Public Affairs team must find means to overcome the bureaucracy that holds up the publication of messages. Insurgents do not care about communication of the truth. Insurgents want

to immediately transmit messages that Americans are killing Afghans out to the Afghan populace. Public Affairs must assist the commander in leveraging the cyber technology for quick message publication of messages to the Afghan populace and limit the beaurocracy causing message delays. The disadvantage to this recommendation is all agencies may not be aware of the publication of the message and may likely disagree with the contents. The risk is, due to increasing the speed to get the true message out first, the message may be inaccurate damaging the trust the coalition desperately seeks to gain from the Afghan populace.

Last, cyberspace is abundantly available to all who desire it. There is no incident or accident that occurs in Afghanistan that is not on a pictured cell phone, camera, or audio device. Coalition forces must be aware that this is happening and ISAF leadership demand that all information technology personnel, civilian or military, layout all system vulnerabilities. To not know the possibility of live drone video being in the hands of insurgents through commercial-off-the-shelf software is unnerving. The disadvantage to knowing the vulnerabilities is the ISAF commander or coalition forces may now second guess the employment of key weapon systems limiting overall capability. The risk with knowing the vulnerabilities and not adjusting is that key and valuable data may fall in the hands of the insurgent. This is a risk the ISAF commander must closely analyze so that the safety of coalition personnel and the Afghan people are not at risk or compromised because of the known vulnerabilities. The commander must fully understand the advantages and disadvantages of each cyber vulnerability and adapt to or overcome before deploying troops or cyber systems into hostile engagements.

Conclusion

Al Qaeda is the first guerrilla movement in history to migrate from physical space to cyberspace.[67] With laptops and DVDs, in secret hideouts and at neighborhood Internet cafes, young code-writing jihadists have sought to replicate the training, communication, planning and preaching facilities they lost in Afghanistan with countless new locations on the Internet.[68] Al Qaeda and Taliban suicide bombers and ambush units in Afghanistan routinely depend on the Web for training and tactical support, relying on the Internet's anonymity and flexibility to operate with near impunity in cyberspace.[69] Cyberspace is a critical enabler for the insurgents to achieve objectives.

The U.S. military is comfortable facing enemies on traditional battlefields, but facing them in the virtual world is a new challenge, said Army Brig. Gen. Susan Lawrence, Joint Staff chief information officer and director of command, control, communications and computers. Until the military figures out how to defeat its adversaries in the operational environment, "we're not going to win the cyber war," she said at a military communications conference.[70] Cyberspace is the new battlefield and unlike past battles where the war was lost with conventional weapons face-to-face, now the trust and confidence of the Afghan people is lost or won by radio broadcasts and news on the Internet. Without a doubt, cyberspace is lethal and extremely challenging to defeat in counterinsurgency operations in Afghanistan.

Endnotes

[1] James J. F. Forest, Countering Terrorism and Insurgency in the 21st Century, Strategic and Tactical Considerations Vol 1, 367 http://books.google.com/books?id=RMUVEw1nfSUC&pg=PA367&lpg=PA367&dq=jihadist+prism+for+viewing+the+environment&source=bl&ots=nJkz-83sQ_&sig=EojcTKH7SJLgJv_-jTMa9Y1JGng&hl=en&ei=hCtWS6qLFMqPlAf16LSTBw&sa=X&oi=book_result&ct=result&resnum=3&ved=0CBQQ6AEwA

g#v=onepage&q=jihadist%20prism%20for%20viewing%20the%20environment&f=false, (accessed October 17, 2009)

[2] "Iraq War Timeline," War Chronicle, http://warchronicle.com/iraq/news/timeline_iraq_war.htm, (accessed January 13, 2010)

[3] Derrick DePledge, War Would Offer New Military Challenges: Goals are More Complex than in 1991Conflict, 15 February 2003, http://www.globalsecurity.org/org/news/2003/030215-iraq01.htm, (accessed December 18, 2009)

[4] Paul McLeary, High-Tech Weapons are Standard Issue for Insurgents, http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=dti&id=news/DTIINSURTECH.xml&headline=High-Tech%20Weapons%20Are%20Standard%20Issue%20for%20Insurgents, (accessed December 16, 2009)

[5] P.W.Singer, Winning the War of Words: Information Warfare in Afghanistan (United Kingdom: Institute of Communications Study, 23 October 2001), University of Leeds

[6] Ibid.

[7] Pfc. Charles Wolfe, PAO Publications (Jalalabad Afghanistan, Jalalabad Air Field, 26 January 2009), Chief of Naval Operations Visits Afghanistan, http://www.cjtf82.com/regional-command-east-news-mainmenu-401/1524-chief-of-naval-operations-visits-afghanistan.html, (accessed November 22, 2009).

[8] Stanley A. McChrystal, ISAF Commanders Counterinsurgency Guidance, http://www.nato.int/isaf/docu/official_texts/counterinsurgency_guidance.pdf, (accessed December 2, 2009)

[9] Joint Publication 1-02, "DOD Dictionary of Military and Related Terms", dated 12 April 2001 and amended through 9 November 2006, and accessible online at http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf

[10] Dr. Dan Kuehl, From Cyberspace to Cyberpower: Defining the Problem, http://www.carlisle.army.mil/dime/CyberSpace.cfm , (accessed November 14, 2009)

[11] Ibid.

[12] See, in roughly chronological order: Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway* 2nd ed. (New York: Thunder's Mouth Press 1996 [first ed. 1994); Ed Waltz, *Information Warfare: Principles and Operations* (Boston, MA: Artech House, 1998); Walter Gary Sharp, *Cyberspace and the U.S.e of Force* (Falls Church, VA: Aegis Research, 1999); Dorothy Denning, *Information Warfare and Security* (Reading, MA: Addison-Wesley, 1998); and Greg Rattray, *Strategic Warfare in Cyberspace* (Cambridege, MA: MIT Press, 2001).

[13] White House, *National Strategy to Secure Cyberspace* (Washington DC: 2003)

[14] During the initial meeting of the task force that wrote this book, representative of the Joint Staff (J6X) effort to develop the National Military Strategy for Cyberspace Operations presented a concept for cyberspace that was clearly unacceptable to virtually everyone in attendance. To

their credit, the J6X team reworked their approach, perhaps influenced by concepts presented by this author at that initial meeting, to the point where the final J6X effort was very similar to that presented during the meeting and to that suggested in this chapter. While this author had some very minor quibbles with the definition in the final product, it comes so close to many of the key points this author offered during the drafting process that we were clearly on the same sheet of music. The same is not true for the 2008 definition of cyberspace signed out by DepSecDef Gordon England.

[15] Christopher J. Castelli, Inside the Air Force (Washington, D.C.: Office of the Air Force, 23 May 2008), Defense Department adopts new definition of 'cyberspace'

[16] Ibid.

[17] James J. F. Forest, Countering Terrorism and Insurgency in the 21st Century, Strategic and Tactical Considerations Vol 1, 370 http://books.google.com/books?id=RMUVEw1nfSUC&pg=PA367&lpg=PA367&dq=jihadist+prism+for+viewing+the+environment&source=bl&ots=nJkz-83sQ_&sig=EojcTKH7SJLgJv_-jTMa9Y1JGng&hl=en&ei=hCtWS6qLFMqPlAf16LSTBw&sa=X&oi=book_result&ct=result&resnum=3&ved=0CBQQ6AEwAg#v=onepage&q=jihadist%20prism%20for%20viewing%20the%20environment&f=false, (accessed October 17, 2009)

[18] Jan C. Morris, Ask the Cyber-Insurgent, 25, www.au.af.mil/info-ops/iosphere/08spring/iosphere_spring08_norris.pdf, (accessed October 3, 2009)

[19] Ibid., 26

[20] Ibid., 25

[21] Ibid.

[22] Glenn Revis, Camera/Iraq: Al Qaeda's in Cyberspace, http://www.camerairaq.com/2005/08/al_qaedas_in_cy.html, (accessed September 13, 2009).

[23] Timothy L. Thomas, Cyberskepticism: The Mind's Firewall,7-8, http://www.au.af.mil/info-ops/iosphere/08spring/iosphere_spring08_thomas.pdf, (accesses November 23, 2009).

[24] Chris Hunter, Eight Lives Down, The Story of the World's Most dangerous Job in the World's Most Dangerous Place, 367, http://books.google.com/books?id=dLnFZz6oWp8C&pg=PT352&lpg=PT352&dq=receipt+of+a+paging+signal+by+phone+is+sufficient+to+initiate+the+IED+firing+circuit&source=bl&ots=HO3fMd1uXB&sig=rT_wZ2EAW8Dz0bSDCm6QsULMzQ4&hl=en&ei=I3VfS9KaONiC8Qab-oiRDA&sa=X&oi=book_result&ct=result&resnum=2&ved=0CAsQ6AEwAQ#v=onepage&q=&f=false, (accessed November 13, 2009)

[25] Thomas L. Friedman, www.jihad.com, http://www.nytimes.com/2009/12/16/opinion/16friedman.html?_r=1, (accessed January 19, 2010)

[26] Glenn Revis, Camera/Iraq: Al Qaeda's in Cyberspace, http://www.camerairaq.com/2005/08/al_qaedas_in_cy.html, (accessed September 13, 2009)

[27] Ibid.

[28] Raja G. Hussain, The Impact of Collateral Damage on the Taliban Insurgency, http://www.au.af.mil/info-ops/iosphere.htm#contact, (accessed November 3, 2009).

[29] Ibid.

[30] Ibid.

[31] Ibid.

[32] Ibid.

[33] The Nation, Taliban Winning Ground in Propaganda War in Afghanistan: report. http://www.nation.com.pk/pakistan-news-newspaper-daily-english-online/International/12-Nov-2009/Taliban-winning-ground-in-propaganda-war-in-Afghanistan-report/, (accessed October 23, 2009).

[34] Ibid.

[35] Ibid.

[36] Ibid.

[37] David Green, Camera/Iraq the War of Images in the Middle east - Al Qaeda's in Cyberspace, August 2005, http://www.camerairaq.com/2005/08/al_qaedas_in_cy.html, (accessed September 28, 2009)

[38] Ibid.

[39] Morris, Ask the Cyber-Insurgent, 25.

[40] Tom Coghlan, The Times: Taleban Spin Doctors Winning Fresh Ground in Propaganda War with Nato, http://www.timesonline.co.uk/tol/news/world/Afghanistan/article6913240.ece, (accessed November 28, 2009)

[41] Greg Grant, Online Defense and Acquisition Journal, McChrystal Troop Boost Comes Friday, http://www.dodbuzz.com/2009/09/24/mcchrystals-troop-request-in-two-days-petraeU.S./, (accessed December 10, 2009)

[42] The Foundry, Taliban Out-Surging U.S. in Information War, http://blog.heritage.org/2009/12/03/taliban-out-surging-U.S.-in-information-war/, (accessed December 8, 2009)

[43] Thomas Friedman, Speaking Out Against Radical Muslims, http://www.nytimes.com/2009/12/23/opinion/l23friedman.html, (accessed January 15, 2010)

[44] Ibid.

[45] General Stanley A. McChrystal, Commander's Initial Assessment, 30 August 2009, 1-1, http://www.globalsecurity.org/military/library/report/2009/090830-afghan-assessment/090830-afghan-assessment-01.htm, (accessed October 9, 2009)

[46] Ibid., D-6.

[47] Ibid.

[48] Walter Pincus, Washington Post: McChrystal Says Insurgents Are Winning Communications Battle, http://www.washingtonpost.com/wp-dyn/content/article/2009/09/26/AR2009092601748.html, (accessed December 9, 2009)

[49] Ibid.

[50] Ibid.

[51] Tom Coghlan, The Times: Taleban Spin Doctors Winning Fresh Ground in Propaganda War with NATO, http://www.timesonline.co.uk/tol/news/world/Afghanistan/article6913240.ece, (accessed November 28, 2009)

[52] Ibid.

[53] Ibid.

[54] Daniel Kimmage, Kathleen Redolpho, Foreign Policy- Iraq's Networked Insurgents, November 2007, http://www.foreignpolicy.com/U.S.ers/login.php?story_id=3999&URL=http://www.foreignpolicy.com/story/cms.php?story_id=3999, (accessed October 2, 2009)

[55] Ibid

[56] Helle Dale, Taliban Out-Surging US in Information War, http://foundry.heritage.org/2009/12/03/taliban-out-surging-us-in-information-war/, (accessed November 11, 2009)

[57] U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, April 12, 2001), 88.

[58] Siobahn Gorman, Yochi J. Dreazen, and August Cole, Wall Street Journal, Insurgents Hack U.S. Drones, December 17, 2009, http://online.wsj.com/article/SB126102247889095011.html?mod=igoogle_wsj_gadgv1& (accessed December 19, 2009)

[59] SkyGrabber Homepage, http://www.skygrabber.com/en/skygrabber.php (accessed December 19, 2009)

[60] Ibid.

[61] Siobahn Gorman, Yochi J. Dreazen, and August Cole, Wall Street Journal, Insurgents Hack U.S. Drones, December 17, 2009, http://online.wsj.com/article/SB126102247889095011.html?mod=igoogle_wsj_gadgv1& (accessed December 19, 2009)

[62] U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, April 12, 2001), 88.

[63] Jeff Harley, U.S. Army Strategic Command G39, Information OPS Division, Information Operations Newsletter, 8-9, www.oss.net/.../20081212%20IO%20Newsletter%20v9%20no%2004.doc, (accessed December 7, 2009)

[64] Ibid, 9.

[65] Ibid, 9.

[66] Hewlett Packard Home Page, http://www.hp.com/sbso/solutions/pc_expertise/article/thinclients_consider.html?jumpid=reg_R1002_USEN (accessed October 3, 2009)

[67] David Green, Camera/Iraq the War of Images in the Middle east - Al Qaeda's in Cyberspace, August 2005, http://www.camerairaq.com/2005/08/al_qaedas_in_cy.html, (accessed September 28, 2009)

[68] Ibid.

[69] Ibid.

[70] Stew Magnuson, Cyber War: Network Vulnerabilities Worry Pentagon, http://www.allbusiness.com/technology/computer-networking-network-security-hacking/867818-1.html, (accessed October 22, 2009)