Cyber Mobilization: A Growing Counterinsurgency Campaign

By Timothy L. Thomas

***Editorial Abstract:** Mr. Thomas analyzes insurgent use of Internet-based forums as a means of recruitment, instruction, and other operational communications. He describes early Coalition counter-cyber efforts in the ongoing Iraq campaign, and outlines recommended changes in US doctrinal and counterinsurgency approaches.*

Introduction

According to US Army publications, two types of offensive actions are key components of insurgency doctrine: armed conflict and mass mobilization. It is clear after more than three years of fighting in Afghanistan and Iraq that the insurgents use improvised explosive devices (IEDs) as their main instrument to conduct armed conflict, and that they have learned to mobilize and conduct conflict-related cognitive activities using cyber means. For example, they capitalize on Internet capabilities to plan, target, educate, recruit, and influence sympathizers. If an insurgency's strength is predicated on the support of the local population, then Coalition counterinsurgency efforts must take cybermoblization—enabled by computerized devices such as cell phones and the Internet—into account.[1]

The warning signs of the advent of mobile phone and Internet mobilization were evident long before the wars in Afghanistan and Iraq. In December 1999, agitators used the Internet to organize resistance to the World Trade Organization (WTO) meeting in Seattle. Net-recruited protestors converged on Seattle from all directions. They frustrated well designed police control plans by using cell phones to move crowds to unattended areas, or to focus on other advantageous spots. Both television and Internet sites picked up coverage of these successful efforts, all of which encouraged similar demonstrations and championed other causes.

The Internet and cell phone have become key insurgency tools due to their ubiquity and mobilization potential. Insurgents in Iraq and Afghanistan have begun to organize online information brigades and online universities. On the Internet, women participate in extremist causes as freely as men, due to the net's anonymity. There is even an Internet site hosting a madrasah: an Islamic institution of higher learning, most often associated with religious teachings.[2] Websites associated with Islamic extremist movements have reportedly grown from twenty, to over 4000, in just five years. Today the spin on Arab specialist T. E. Lawrence's 1920 idea that "the printing press is the greatest weapon in the armory of the modern commander" [3] would be: "the Internet is the greatest weapon in the armory of the modern extremist."

To put it bluntly, it appears that a group of insurgents, without any formal theoretical and doctrinal IO background, has successfully confronted well-organized, well-financed US and Coalition IO forces. For example, the US has an IO Corps, IO doctrine, IO magazines, IO courses in military institutions, and so on. US forces are often hampered by a lengthy chain of command approval process that takes hours or days to grant approval. The insurgency's cybermobilization focus (manipulate public opinion, mobilize fighters, and recruit suicide bombers, among other uses), without such chains of command or even laws, indicates the US counterinsurgency (and IO) definitions need to be more responsive.[4] By excluding cyber activities, the definition misses a key insurgent capability, which acts in an independent or integrated fashion to mobilize the population. Excluding cyber activities ignores a key motivator behind one of insurgency doctrine's two key components: mass mobilization.

Past Versus Present

In 1991, during Operation Desert Storm, CNN was the only comprehensive news outlet available worldwide. Fifteen years later, in addition to a broader range of international news services, there are a multitude of insurgent websites offering images, directives, and testimonials that compete for the minds and emotions of Iraqis, Afghanis, and for world opinion. These websites take advantage of the societies' prejudices and beliefs, attempt to recruit the disadvantaged, and espouse extremist points of view. For the most part, these sites are anti-Coalition and try to drive a wedge between legitimate Iraqi or Afghan police or military forces, and the Coalition.

Insurgents cyber mobilize in two primary ways. First, they use the Internet to respond to unfolding events before Coalition forces have a chance or opportunity to respond. As a result, Coalition forces are often blamed for actions the insurgents committed. Second, the Internet is used to post influential information items to include extremist training materials, an ideological rational for actions, instructional manuals, plus propaganda and agitation materials. Some have used creative methods. For example, a recent posting to a jihadi webpage announced a competition to design a new website for an Iraqi militant group. The motivating prize was a chance to fire remote controlled missiles at a US military base.[5]

To counter the impact of these websites, US brigade commanders and other Coalition leaders often developed

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyber Mobilization: A Growing Counterinsurgency Campaign	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Foreign Military Studies Office,Fort Leavenworth,KS,66027**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**6**	

appropriate IO actions on the fly. Much of this was done in the absence of an adequate information operation (IO) "quick response" template (IO is one of the designated concepts to counter insurgent information actions). Lieutenant General David Petraeus, commander of the Combined Arms Center at Fort Leavenworth, noted at a recent IO conference that the key is *speed*.[6] Coalition forces need to respond to a situation by providing information to the population before the insurgents can act. Historically, Coalition forces do not receive much—if any—training on this issue.

Them—What the Insurgents Do With Cyber Capabilities

Insurgents interpret and use cyber-generated information and actions differently than US operators. This is because an insurgent's decision-making context itself is very different. They have no need to adhere to any law other than their own strict interpretation of the Koran, they use a jihadist prism for viewing the environment, and their indifference to killing innocent people allows them to intimidate, influence, and mobilize their believers in ways unacceptable to civilized commanders. Successful insurgents cybermobilize, cyberrecruit, cybermanipulate, cyberrespond, and cyberexploit modern conflicts faster than their opponents. Prior to his death, Iraqi al-Qaida leader Abu-Mus'ab al-Zarqawi used the Internet to speak about US casualties, the Iraqi elections, Israel, and other issues. He also used the Internet to show the preparation and execution of an attack on a hotel complex in Baghdad. The Mujahideen Army posted a video titled "The Sniper of al-Fallujah." Such messages are often the persuasive and convincing element that influences ideological or religious fence sitters to adopt extremist causes.

The Web also recruits suicide bombers from among these undecided. Terrorist authorities Scott Atran and Jessica Stern note that extremist websites play a key role in forging the mind set of a suicide bomber. The Net provides a

Al-Qaida on the Web (SITE.org)

way to bond individuals with the cause, and provide them direction as they surf jihadi websites. The US and Coalition need to provide a similar positive counter website, whether it be alternatives for those who might succumb to the recruiters, or simply counters to these negative influences.[7]

Insurgent use of the cyber element has introduced an operating pattern different from the well-known US military procedure, the OODA loop. This latter concept is based on author John Boyd's paradigm to observe, orient, decide and act (OODA). His model determined a method for identifying and targeting an opposing force that worked well in the Cold War environment. As a US Air Force pilot, Boyd had time to utilize all four elements as he flew missions. This paradigm works in Iraq and Afghanistan when Coalition forces confront insurgents face to face, such as in the fight for Fallujah. However, the invisible enemy often takes the initiative in both conflicts.

We may not know who or where the adversary is. Insurgents hide, and may initiate confrontation by remote control, as seen with improvised explosive devices (IEDs), without ever confronting Coalition forces. Only after an insurgent-generated incident does/can our forces react. Given this scenario, Coalition troops cannot observe and orient—they must decide and act. The invisible enemy has stolen the key elements of observation and orientation. And in many instances, Coalition forces must process the action and perform policy coordination before acting.

Insurgents use a different paradigm. They initiate a physical action and then immediately cyber respond, whether it be cell phone, the Internet, or some other device. This physical action, information, response (PAIR) loop allows them to be first with a version of a story, reaching an audience with whom they have some credibility—and which offers them influence and support. This virtual dimension allows them to manipulate an event before Coalition forces can react.

US Army Colonel Rob Baker, a former Brigade Commander in Iraq, provided a battlefield example of the PAIR paradigm. He stated in one instance an insurgent suicide bomber detonated his belt too early and killed a number of Iraqis, narrowly missing his intended US target. Baker noted it was vital for US forces to immediately distribute suicide bomber/IED "handbills" telling Iraqis what had happened.[8] Before we could send information up the line to create the handbills, insurgents beat our forces to the information punch, stating the US launched a missile strike on the Iraqi populace. An anti-American crowd soon appeared, threatening to riot. While it is not known for certain if instigators used a cyber device to rally the crowd, the assemblage itself would be reported on some cyber devices. Meanwhile, our forces were properly running the incident through channels and awaiting word on what to do next. The insurgents used the PAIR model to perfection, even gaining advantage from a failed operation.

Press reports indicate Coalition forces are now less concerned with an insurgent's use of viruses and other malware than with these cyber-related issues of mobilization and manipulation. Even the US Federal Bureau of Investigation (FBI) noted terrorist groups lack the ability to damage the US via an Internet-based attack.[9] Thus, the incredible force the US assembled to protect its information security is working well. But we have not done nearly as well at anticipating insurgent use of other cyber capabilities. On 9 August 2005, the *Washington Post* noted the Web is a weapon for insurgents in several ways. They use it to:

- Intertwine real-time war with electronic jihad

- Immortalize suicide bombers
- Taunt the US military
- Release tactical details of operations many times each day
- Publish a monthly Internet magazine and
- Negotiate with bin Laden. [10]

By utilizing the Web in this manner the insurgents have become very effective, with a far smaller staff and less effort than Coalition opponents employ. Extremist websites now compete with global news agencies for media attention in Iraq and Afghanistan. There is no need for rationality or balanced news coverage on their sites. Insurgents are only interested in attracting true believers to their cause, and not in convincing someone of their politics. Insurgent audiences may not be as large as the population they are fighting, but they can be far more committed.

The increase in the number of jihadi websites has allowed the insurgency to grow like a virus and act intuitively. Websites enable insurgents to discuss their tradecraft and to exchange justifications for actions, both accomplished and planned. To add veracity to their claims they often include video clips as an integral part of their online activities. To Islamic extremists, the Internet is not a place to publish open source material, it is a place to conduct open source warfare.[11] Some extremists believe the Internet battle for influence and persuasion is second only to physical confrontation. A 28 November 2005 posting on the al-Safinat forum site noted the following:

> *"There is no doubt that the jihadi forums play a critical role in providing aid to the mujahideen on the battlefield. Who could have thought that it would break the ring of steel that the Crusaders and Jews have attempted to erect in order to conceal the voice of the jihad, and cover up their humiliations on the battlefield?"* [12]

A Web statement from Minbar Ahl al-Sunna wal-Jama'a, posted in March 2005, noted formation of an Information Jihad Brigade. Note this is not an IO brigade, it is just an information brigade without the operations designator. It is composed of design, language, and publication divisions. The brigade's aim is to conduct a full-scale propaganda war to "influence the morale of our enemies." In December 2005, the Middle East Media Research Institute reported insurgents are using Yahoo.com as a gateway for indoctrination and incitement of aspiring insurgents.[13] Perhaps this gateway is a product of the information brigade? A year later, in March 2006, the Al-Rashedeen Army posted an open letter to President Bush on the Internet. The group's operations director read the letter in English, asking questions concerning US atrocities, and ending by suggesting President Bush think over the fact that "God is on our side, and always will be."[14]

Websites also allow Muslim extremists to spread targeting information. An individual known as "al-Mohager al-Islami" ("The Islamic Immigrant") has been posting messages to tens of e-group forums, both public and password-protected, about the locations and equipment of US and British sites in Kuwait, Qatar and other areas. These postings include photos of embassies and living areas. Besides posting the introductory message, Al-Mohager al-Islami provides logistic information about several bases in Iraq, and calls upon mujahideen to target these sites. Thus, the Net serves as an intelligence and reconnaissance asset for extremists, even in the planning stages of armed conflict. Al-Mohager al-Islami also provides a nearly 40 page pamphlet titled *The Art of Kidnapping – The Best and Quickest Way of Kidnapping Americans.* The manual includes information for planning raids, the composition of support crews, general rules for crews to follow, observation points, kidnapping suggestions, and methods of capturing Americans. [15]

Insurgent Targets

Insurgents have different targets in mind when developing Internet messages. In some cases the main cyber mobilization targets appear to be the minds of humiliated or resentful Muslim emigrants. A 23 January 2006 video product from the Global Islamic Media Front entitled *Jihad Academy* vividly demonstrates this point. A voice at the start of the video recites, "the roots of humiliation cannot be removed except with the showers of bullets. Without the spilling of blood, dishonor cannot be wiped off the forehead." [16] Once recruited, insurgents offer new recruits actual targets, especially oil installations or US infrastructure, via the Net. [17]

Insurgent use of the Internet for such targeting purposes represents a significant change in how we perceive and understand warfare, especially among the general population. One conclusion is that the Internet and associated websites may be the second most important insurgent force multiplier (IEDs remain number one). It enables insurgents to shape and influence local popular opinion, thereby manipulating the perceived outcome of coalition operations through the Web. No such resource was ever afforded insurgents in the past. Coalition counterinsurgency plans to limit this capability require extreme sensitivity to local customs, values, and beliefs, as well as an understanding of both insurgent Internet operating procedures and methods to counter them.

US—What American and Coalition Forces Do With Information

The US military establishment would label most of these insurgent activities that involve the use of the Internet as information operations. Joint Publication 3-13, *Information Operations*, 13 February 2006, defines IO as:

The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. [18]

This same publication defines only one cyber-related term: "cyberspace." The US Army's November 2003 Field Manual 3-13, *Information Operations* declares the term information operation (IO) has five categories: psychological operations, operational security, computer network operations, military deception, and electronic warfare. A proposed Army definition of IO:

Actions taken by forces and individuals to affect attitudes, behaviors, information systems, and information while protecting one's own through the integrated employment of the capabilities of electronic warfare, computer network operations, psychological operations, military deception and operational security in concert with specified supporting and related capabilities throughout the information environment. [19]

Both the Joint Publication and the Field Manual on focus on attitudes, behavior, and decision-making, indicating their emphasis is clearly not on the sort of counter capabilities required to offset insurgent cybermobilization. One would expect to see "counterpropaganda," or a similar term in either publication. In fact, this expression appears only twice in Joint Publication 3-13, both times in Appendix B. A graph lists counterpropaganda under IO and Public Affair columns, but the term is not included in the glossary. Clearly these documents attach little importance to the concept. Alternately, the terms counterintelligence and countermeasures, are used often.

Before US forces entered Iraq in March 2003, they methodically prepared the proposed information battlefield based on traditional IO capabilities and principles. Then, the battle for Baghdad ended abruptly. Understandably, they conducted little long range IO planning, since US forces expected the city fight would last for days. As a result, we had few assets available to know what was being broadcast on the city's fifteen radio stations, satellite TV networks, and in newspapers. Further, this was the first time our forces had encountered an information environment in an enemy city of this size. A new phase of intensive IO planning ensued. IO teams took to the challenges, which grew even more rapidly as insurgent activities proliferated.

US Army Reserve Captain Bill Putnam headed the Coalition's early Open Source Intelligence effort in Iraq, including the *Baghdad Mosquito*, a document which reported the latest Baghdad street rumors. Putnam's comments on initial efforts indicate US IO and public affairs doctrine in Iraq were focused on making the Iraqi information environment conform to US doctrine. Rather than allowing the environment to determine how we would conduct IO, early actions focused on fitting the guidance.[20] This is a huge problem according to Putnam, since

The all-important "word on the street" (Defense Link)

he believes "it is virtually impossible for a counterinsurgency campaign to be successful without some level of the local population's support."[21] Putnam therefore identified "how" the Iraqis receive information and formulate opinions as the most important IO consideration. Iraqis get the word via satellite television channels, one's family and friends, the street (rumors), religious figures, and newspapers. Putnam believed we had to target this "circle of influence" to conduct successful IO. The doctrinally-based template did not correspond to the reality on the ground—a reality strongly influenced by cultural factors. Fortunately, US and Coalition forces have since responded aggressively to this oversight. Cultural factors are now an intense focus of armed forces time and planning, and IO planning shows renewed creativity.

At the December 2005 IO conference at Fort Leavenworth, Colonel Baker stated intelligence and IO were the two most important aspects of the fight. He confirmed the necessity of developing practical solutions to the IO challenges his brigade faced in Iraq, and the need to go beyond relying solely on doctrine. Further, he felt it necessary to bypass IO doctrine on several occasions, and use his staff's creativity when the situation required. Baker noted "information operations have to be more than a plan on a piece of paper. You have to have the ability to operationalize it and make it important to all of your leaders, so they embrace it and integrate it into everything they do."[22]

Colonel Baker developed an information battle rhythm matrix that required him and his staff to perform specific information-oriented events on specific days of the week (meetings with the media, local leaders). Not only did this enable him to keep his finger on the information pulse of the insurgency, it allowed local media and culture integration into the IO plan. Colonel Baker also became a strong proponent of the quick-reaction handbill that would offer a Coalition explanation of an action. This often allowed his forces to beat the insurgents to the information punch.[23]

Thus, traditional ways of conducting IO business in Iraq were helpful, but had to be supplemented with other measures. Commanders who were focused on maintaining an influence advantage had to create responses on the fly, based on situations they encountered. Still, US forces require a vetting process, to understand an event before responding. Though slow, this is a necessary response mechanism, because it helps ensure insurgents aren't manipulating Coalition forces. Too slow of a response gives insurgents time to develop a virtual force multiplier, by providing the populous a culturally astute version of an event, modified to the insurgents' benefit. This

enables a group of insurgent website designers and Internet responders to influence the population much to the same extent as the Coalition's highly organized and financed IO efforts. Again, we must develop countercyber capability for the IO lexicon and action toolkit.

It is important for planners to begin conceiving a virtual insurgency environment, because it can influence an operation to the same degree as a radio transmission, by summoning troops to the front. Working on countercyber capabilities now allows US IO planners to understand how to neutralize future insurgent cyber capabilities.

British military expert John Mackinley's concept of the "virtual arena of war" sees a new type of insurgency emerging, in which the virtual element will play a major role. He notes "The global insurgents that oppose the international Coalition can be characterized as a complex insurgency; they grow organically and exist in considerable depth beyond the operational area."[24] He further states "A complex insurgency grows organically like a virus and acts intuitively. To defeat it may require reorganized security structures and an unfamiliar modus operandi."[25]

One must be careful not to overlook the virtual aspect of this complex, growing virus. The virtual arena can operate in considerable depth beyond the operational area (in fact, it can operate all over the globe), while simultaneously resting in insurgent hands at the tactical level.

Conclusions

We should not confuse the virtual dimension with information warfare. This dimension must be regarded as an arena no single party controls; therefore is it not a special weapon exclusively in the hands of any particular user. Just as friendly and enemy forces act against each other in strategic and operational spaces, so they do in the virtual dimension.[26]

Mackinley believes the virtual dimension's proliferation of actors has created another theater of war, with key objectives and tactical areas seizeable by either side. Further, he notes counterstrategy must contain interconnected strategic, operational, and virtual dimensions.[27] This arena is turning PSYOP into "CYOP," a cyber-enabled psychological mobilization and recruitment factor. The recent capture of an Internet hacker who was also an Al-Qaida conduit underscores this fact. A young webmaster who called himself "Irhabi 007" helped propel "the jihadists into a 21st Century offensive through his ability to covertly and securely disseminate manuals of weaponry, videos of insurgent feats such as beheading, and other inflammatory material." Earlier he had joined a password-protected forum used for issuing military instructions, propaganda, and recruitment.[28]

Noted author Hans Magnus Enzenberger stated over ten years ago that the nature of war was changing from "purposive, ideologically driven enterprises undertaken by highly organized industrial powers" to "molecular civil war."[29] Insurgent tactics in Iraq and Afghanistan appear to fit Enzenberger's description.

However, the Internet offers a new spin to Enzenberger's molecular civil war theory. Insurgents have gained an ideological and motivating force multiplier, since the Net encourages and supports the "will" of the fighter through culturally-attuned images and messages. At the same time, their operating principles (individual acts of terror by people who blend in with the population) take away or neutralize many Coalition multipliers such as its high-technology advantage.

While insurgents are culturally attuned to the needs and desires of the population, Coalition forces have a limited frame of reference for understanding the world playing out around them. They have increasing difficulty monitoring and analyzing the plethora of sites available to insurgents and their sympathizers. The Internet allows extremists to produce a cacophony of responses to actions they take, or mistakes the Coalition makes. Websites are sure to produce some messages that ring true with some portion of the population. It is here insurgents generate much support, and Coalition forces must do as much as possible to counteract this capability. The US and its Coalition partners have ventured into this battlespace, but not with the same degree of precision and confidence as they do on a traditional hot battlefield.

Commanders recognize this, as well as the need to act more creatively when attempting to manage the cyber/information problem. They have implemented plans on their own in many cases, as Colonel Baker's experience indicates. Noted military journalist Ralph Peters agrees, stating "counterinsurgency warfare is the realm of the officer who can think beyond the textbook, who thrives in the absence of rules."[30] Understandably, doctrine writers have trouble keeping up with the pace of change technology thrusts upon us.

We must develop new and different IO tools or mindsets. US IO specialists need to study the cyberinsurgent communities' Internet's use, and learn to focus on "how" the circle of influence works in a particular culture: what images matter? IO specialists should develop "countercyber" plans and actions, as well as an understanding of resulting consequences. As a result, we must modify the term counterinsurgency as currently defined, to deal with this new issue.

Lenin rewrote Clausewitz for the class and ideological struggle, and the West adapted the same works in conducting the Cold War.[31] The current situational context—religious backdrop—requires Coalition forces to adapt once again. Virtual elements are the agitators and propagandists of this new form of "class/insurgent warfare." If extremists are responsible for providing radical Islam with strategic depth, then the Internet fuels the ideologically-driven insurgency.[32] Counterinsurgency doctrine will be shortchanged if it doesn't consider the virtual arena, and add that element to its definition. Past insurgencies did not have an Internet to cybermobilize people, as do today's insurgents. Fine-tuning our definitions, and enhancing our understanding of

cyber mobilization, will hopefully make us more aware and adept at neutralizing this virtual arena of war.

Endnotes

[1] It is hard, if not impossible, for Internet viewers to make distinctions among insurgent groups. Neither the Internet source nor the web creator's attributes are often known with certainty in the virtual arena of war.

[2] Injy El-Kashef, "Islam Dot Com," *Al-Ahram Weekly*, 20 October 2005. Spelling and initial part of the definition of madrasah taken from Wikipedia online.

[3] T. E. Lawrence, "The Evolution of a Revolt," in *The Army Quarterly and Defense Journal*, October 1920, pp. 55-69 as cited in The Foreign Area Officer Association's Internet publication (http://www.faoa.org/journal/telawl.html), quote taken from "T. E. Lawrence and the Establishment of Legitimacy during the Arab Revolt," by Kevin J. Dougherty, downloaded 1 March 2006.

[4] Counterinsurgency is defined as "those military, paramilitary, political, economic, psychological and civic actions taken by a government to defeat insurgency." See Joint Publication 1-02, *Dictionary of Military and Associated Terms*, 12 April 2001 as amended through 31 August 2005, p. 127.

[5] Sebastian Usher, "Militants' New Tack in Cyber War," BBC News, downloaded 5 December 2005 at http://news.bbc.co.uk

[6] Jeff Crawley, "Proponent Hosts Info Ops Gathering," *The Lamp*, Fort Leavenworth, Kansas, 22 December 2005, p. 1.

[7] Scott Atran and Jessica Stern, "Small Groups Find Fatal Purpose through the Web," *Nature* 437, 29 September 2005, downloaded from http://www.nature.com/nature/journal/v437/n7059/full/437620a.html

[8] Crawley.

[9] ZDNet News, 7 December 2005, at http://news.zdnet.com. US information expert John Arquilla disagrees with this assessment, noting that "the terrorists are preparing to mount cyberspace-based attacks, and we are ill prepared to deal with them." See URL:http://sfgate.com/cgi-bin/article.cgi, 15 January 2006.

[10] Susan B. Glasser and Steve Coll, "The Web as Weapon," *Washington Post*, 9 August 2005 as downloaded from the Internet on 28 October 2005.

[11] Term used by John Robb to describe insurgents' use of the Internet.

[12] Stephen Ulph, "The Global Jihad's Internet Front," in *Terrorism Focus*, The Jamestown Foundation, Volume II, Issue 23, 13 December, 2005.

[13] "Terrorists Using Yahoo.com," WorldNetDaily.com, posted 6 December 2005.

[14] SITE Institute, 26 March 2005, "Al-Rashedeen Army Presents," http://siteinstitute.org/bin/articles.cgi?ID=publications160306&Category=publications&Subcategory=0

[15] SITE Institute, 22 December 2005, located at www.siteinstitute.org. Some examples of other jihadi manuals on a variety of issues are at:

http://www.geocities.com/tadrebatfialjihad10/COLT-45.zip

http://www.geocities.com/tadrebatfialjihad10/katem00721.zip

http://www.geocities.com/algazairiyat_00768/dawrat.zip

[16] www.jaami.com/vb/showthread.php, downloaded from the FBIS website and reviewed on 25 January 2006.

[17] Stephen Ulph, "Internet Mujahideen Intensify Research on US Economic Targets," in *Terrorism Focus*, the Jamestown Foundation, Volume III, Issue 2, an Internet product. See http://www.Jamestown.org.

[18] Joint Publication 3-13, *Information Operations*, 13 February 2006, p. GL-9.

[19] Crawley.

[20] Bill Putnam, "Winning Iraqi Hearts and Minds," *Army*, January 2005, p. 7.

[21] Ibid., p. 8.

[22] Crawley.

[23] Author's understanding of Colonel Baker's operational concept offered at the December 2005 Fort Leavenworth IO conference.

[24] John Mackinley, *Defeating Complex Insurgency*, The Royal United Services Institute, Whitehall Paper 64, 2005, p. xii.

[25] Ibid., p. vi.

[26] Ibid., p. 13.

[27] Ibid.

[28] Rita Katz and Michael Kern, "Terrorist 007, Exposed," *Washington Post*, 26 March, 2006, p. B1.

[29] Hans Magnus Enzenberger, *Civil Wars: From LA to Bosnia*, New York: New Press, 1994.

[30] Ralph Peters, "No Silver Bullets," *Armed Forces Journal*, January 2006, p. 39.

[31] See Jacob W. Kipp, "Lenin and Clausewitz: The Militarization of Marxism, 1915-1921," Soviet Military Doctrine from Lenin to Gorbachev, 1915-1991, edited by Willard C. Frank, Jr., and Philip S. Gillette, Greenwood Press, 1992.

[32] Warren Bass, "Off Target: American's Foundering War on Terror," *The Washington Post Book World*, 6 November 2005, p. 3.

Tim Thomas, LTC, US Army, Retired, served as a Soviet/Russian Foreign Area Officer. His assignments include brigade S-2 and company commander in the 82d Airborne Division, and the Army Russian Institute. He has done extensive research and publishing in the areas of peacekeeping, IO, and PSYOP. He currently serves as a Senior Analyst in the Foreign Military Studies Office, Ft Leavenworth. He holds a BS from West Point, and Master of Arts from USC.