CHAPTER 18

CYBER MOBILIZATION: THE NEGLECTED ASPECT OF INFORMATION OPERATIONS AND COUNTERINSURGENCY DOCTRINE

Timothy L. Thomas

For over two years, the U.S. armed forces have focused on seeking ways to counter insurgent use of improvised explosive devices (IEDs) in both Afghanistan and Iraq. Less attention has been paid to countering the mobilization process that produces the seemingly unending line of insurgents willing to (1) become suicide bombers (walking IEDs, or WIEDs), (2) prepare the IEDs, and (3) fight street battles. The insurgents use the Internet's "cyber mobilization" potential to fuel and supply this line of volunteers. They have been particularly successful in recruiting volunteers from other countries such as Saudi Arabia and Egypt.[1] This success has forced coalition forces to continually react to the environment instead of controlling it.

According to U.S. Army publications, two types of offensive actions are key components of the insurgency doctrine: armed conflict and mass mobilization. It is clear that the insurgents use IEDs as their main instrument to conduct armed conflict. It is just as clear that they have learned how to mobilize and conduct conflict-related cognitive activities using cyber capabilities. Coalition forces have reacted to the former with speed and money. IED study groups have proliferated. Coalition forces have responded to the latter mobilization concept with an ill-equipped concept, information operations (IO). Fighting IEDs with artillery is akin to fighting cyber mobilization with U.S. IO paradigms.

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **2007**	2. REPORT TYPE	3. DATES COVERED **00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE **Cyber Mobilization: The Neglected Aspect Of Information Operations and Counterinsurgency Doctrine**	5a. CONTRACT NUMBER
	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) **Army Training and Doctrine Command,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

This article was previously published as a chapter in a three volume set titled Countering Terrorism and Insurgency in the 21st Century, volume 1, edited by James J.F. Forest, published by Greenwood Press. Publication: 6/30/2007

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**22**	

Insurgent cyber mobilization capabilities are designed to conduct psychological warfare activities, to propagandize insurgent successes and counter coalition allegations, and to recruit, finance, and train more fighters. Insurgents designate public affairs specialists to be their spokespersons and establish video production centers to promote their cause. During congressional testimony in early May 2006, one report noted that "al Qaida has advertised online to fill jobs for Internet specialists, and its media group has distributed computer games and recruitment videos that use everything from poetry to humor to false information to gather support. The media group has assembled montages of American politicians taking aim at the Arab world."[2] IO, on the other hand, doesn't even recognize the cyber mobilization concept. In fact, IO is devoid of cyber terminology in general, other than the term cyberspace, and it nearly ignores the concept of counterpropaganda.

If an insurgency's strength is predicated on the support of the local population, then coalition IO and counterinsurgency efforts must take cyber mobilization (mobilization enabled by computer chip-driven devices such as cell phones, the Internet, compact discs [CDs], and so on) into account.[3] A "counter cyber mobilization" strategy should be contemplated to assist in controlling the environment, and a new doctrinal section on cyber mobilization should be developed for U.S. IO and counterinsurgency manuals. Cyber mobilization is a problem that will be with us for a long time.

This chapter will discuss the precedents to the current use of the Internet in Iraq and Afghanistan; the U.S. IO paradigm problem and its extension into understanding the virtual aspect of an insurgency; the use of the Internet by insurgents in Iraq and Afghanistan; and coalition countermeasures to insurgent efforts. The chapter will then conclude with some relevant recommendations for U.S. IO and the counterinsurgency doctrine.

PRECEDENTS

Communication devices have long been an important means of facilitating an uprising. The French Revolution witnessed the radicalization, education, and organization of the populace in large part due to the power of journals, newspapers, pamphlets, printers, and publishers. The latter communication devices were particularly effective at the time of the deregulation of the French press, when there were no rules on copyright, no rules on publications, and no libel laws. Today, gangs, terrorist groups, insurgents, and other hate groups use the Internet and cyberspace under similar conditions.[4] Audrey Kurth Cronin notes that blogs are today's revolutionary pamphlets, Web sites are news dailies or TV stations, list servers are broadsides, images are projected like caricatures or symbolic pictures of the past, and every item is passed faster than ever before and is available 24/7. The Internet is creating identity and a sense of unity, building a cause-driven conscience, and returning segments of the populace to mob-driven feudal forms of warfare.[5]

Cronin adds that the Internet is different from past propaganda methods in that it can demonstrate the ruthlessness and power of an insurgency in ways not available to former communication devices. By crafting their version of events, insurgents can inspire more violence. Videos showing insurgent attack successes and the publication of fiery speeches impart a tremendous emotional appeal to potential insurgents.

Ben Venske, a specialist in jihadi videos, has noted that such videos can be divided into seven divisions or purposes: production videos (1–2 hours in length, with a wide range of source material); operational videos (short, quick clips of attacks, typically 1–8 minutes); hostage videos (tools in ongoing operations, which increase attention on a group); statement videos (featuring mid to senior tiers of a group and intended for morale boost, recruiting, fundraising, and political positions, often released to media as well as the Internet); tribute videos (when significant group members or large numbers are killed); internal training videos (usually not intended for the public); and instructional videos (how to accomplish a specific skill).[6] The videos as a whole impart a type of follow-on psychological attack on viewers, since they amplify attack effects and demonstrate success, according to Venske.[7]

Cronin and Venske's comments indicate that the warning signs of the advent of the cell phone and Internet mobilization of the population were evident long before the wars in Afghanistan and Iraq. They were even evident in the United States. In December 1999, the Internet was used to organize resistance to the World Trade Organization (WTO) meeting in Seattle. Internet-recruited protestors converged on Seattle from all directions. They frustrated well-designed police control plans by using cell phones to move crowds to areas left unattended or to focus on other advantageous spots. Both television and the Internet picked up coverage of these successful efforts that encouraged similar demonstrations elsewhere utilizing the same technologies to champion various causes.

Thus the Internet, and to a lesser degree CDs and cell phones, have become key insurgency tools due to their ubiquity, cyber mobilization potential, and anonymity. Women can participate on the Internet at little risk, even in male-dominated societies, since they appear anonymous. There is even an Internet site hosting a madrasa (Islamic school).[8] Web sites associated with jihadist movements reportedly have grown from 20 to over 4,000 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"[9] would be that "the Internet is the greatest weapon in the armory of the modern jihadist."

Gabriel Weimann, one of the most well-known authors on the use of the Internet by terrorists and insurgents, noted that the Internet allows groups to challenge a state's media domination of political discourse and even its political culture. It also permits interaction among elements to an extent never before contemplated (via e-groups, chat rooms, forums, online magazines, message boards, and online manuals), and it allows for extensive targeting (potential supporters, enemies, international public opinion, and journalists).[10]

Internet broadcasts also have a tremendous psychological appeal that is often overlooked. Videos or statements have generated a stimulus and response pattern among insurgents and audiences, according to Weimann, that includes both supporters and nonsupporters alike. A conditioned reflex is generated when statements are made about potential violent actions that cause anxiety in the audience.[11] Further,

> From a psychological perspective, two of the greatest fears of modern times are combined in the term "cyberterrorism." The fear of random, violent victimization blends well with the distrust and outright fear of computer technology. An unknown threat is perceived as more threatening than a known threat. Although cyberterrorism does not entail a direct threat of violence, its psychological impact on anxious societies can be as powerful as the threat of terrorist bombs.[12]

Weimann notes that the biggest obstacles to our understanding the actual threat of cyberterrorism are a fear of the unknown and a lack of information or, worse, too much misinformation.[13]

It should be highlighted that the Internet is also fostering future generations of insurgents through the spread of hate propaganda aimed primarily at Jews and Christians. For example, the Web site www.memritv.org has hosted cartoons from Hizbollah[14] TV that show Jews turning into animal forms. The computer game *Special Forces* was developed by the Hizbollah Central Internet Bureau. It places players in operations against Israelis, based on actual Hizbollah battles with Israeli forces.[15] It is a violent game that praises martyrs and gives credit to players who shoot Israeli politicians and others.[16]

The Hamas site al-Fateh (The Conqueror) discusses jihad, science, and tales of heroism. The site also posts messages promoting suicide terrorism.[17] Other sites, which host photos and videos of jihadi summer camps for kids, display images of young Arab children dressed as suicide bombers, while others conduct mock beheadings. Such programs for children are very likely to produce at least a few future insurgents because of their contribution to what Stanford psychologist Albert Bandura refers to as "moral disengagement." In order for individuals to become lethal terrorists, according to Bandura, they must acquire an ability to sanctify harmful conduct as honorable and righteous, which is achieved by moral justification, exoneration of comparison with graver inhumanities, sanitization of language, displacement of responsibility, and dehumanization.[18]

Similarly, psychologist Anthony Stahelski's research led him to develop a model of social psychological conditioning through which individuals are conditioned to identify a group's enemies as evil subhumans or nonhumans who should be killed.[19]

Al-Arabiya, an Arabic language television news channel located in Dubai, offered a view of the Internet's impact on youth from director Abd al-Rahman al-Rashed. He noted that the videos of Iraq's former al Qaeda insurgent leader, Abu Musab al-Zarqawi, have been "broadcast directly over the Internet to hundreds of thousands of youth who see and hear and read most of their information from it . . . Most of the terrorist crimes are tied to the Internet as the preferred theater."[20] Al-Rashed's comments are frightening if true.

U.S. PARADIGM PROBLEM

The U.S. military would label most of these insurgent activities that involve the use of the Internet as "information operations." The U.S. Armed Forces *Joint Publication 3-13, Information Operations* (published February 13, 2006) defines IO as "the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations (PSYOP), 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."[21] It is important to note that the *Joint Publication* only defines one cyber-related term—cyberspace. This relative lack of attention toward cyber-related terms, and their absence from IO and the counterinsurgency doctrine, is a secondary focal point of this chapter, close behind the emphasis on cyber mobilization as an overlooked modern phenomenon.

Other armed forces publications reflect much the same attitude. The U.S. Army's November 2003 *Field Manual 3-13, Information Operations* declares that the term information operations has five categories of activity: PSYOP, operational security, computer network operations, military deception, and electronic warfare. The term also includes specified supporting and related capabilities. A newly contemplated U.S. Army definition of IO states that it is "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, PSYOP, military deception and operational security, in concert with specified supporting and related capabilities throughout the information environment."[22] The focus of both the *Joint Publication* and the *Field Manual* on attitudes, behavior, and decision making indicates that their emphasis is clearly not on developing the capabilities required to offset an insurgent's cyber mobilization process. In fact, in the *Joint Publication,* the term "counterpropaganda" is used only twice (in an appendix and not the main text), and it is not included in the glossary. The terms counterintelligence and countermeasures, on the other hand, are used often.

The Internet has clearly become a weapon of mobilization that is interactive, fast, and cheap, with few (or, as in the insurgent's case, zero) regulations or laws to control it. To put it more bluntly, the Internet has allowed a group of insurgents, without any formal theoretical and doctrinal information operations background, to successfully confront a colossal U.S. and coalition IO force that is not only well organized (the United States has an IO Corps, IO doctrine, IO magazines, IO courses in military institutions, and so on) but also well financed. With thousands of IO personnel, former Secretary of Defense Donald Rumsfeld sounded mystified when observing that "the extremist groups are able to act quickly on the information front, with relatively few people, while the U.S. government bureaucracy has yet to keep up in an age of e-mail, web logs and instant messaging . . . We in the government have barely even begun to compete in reaching their audiences."[23]

This is quite a damming statement for a country that invented the Internet. The overwhelming implication is that U.S. PSYOP and computer network operations need refinement or greater elucidation to take into account cyber-related terms, a concept that is ubiquitous in civil society. Why cyber-related terminology hasn't made its way into the military lexicon is a mystery. There are now hundreds of cyber-related terms and concepts in online dictionaries. One surmises under such circumstance that the military is a prisoner of sorts to its own IO paradigm and sound bytes.

Including cyber terminology in IO and the counterinsurgency doctrine is now a necessity, since the military and civilian worlds have been drawn much closer together by the Internet. The interaction of the military and civilian worlds is inherent in the idea of insurgent warfare. Such was not the case in 1991 during Operation Desert Storm, when two military forces confronted one another. At that time, *CNN* was the only comprehensive news outlet available worldwide. Now, just 15 years later, in addition to a much broader range of international news services, the battle for influence rages in numerous cities between militaries, insurgents, and civilians. There are a multitude of insurgent Web sites taking advantage of this environment, offering images, directives, and testimonials that compete for the minds and emotions of the local populace and world opinion. These Web sites take advantage of the prejudices and beliefs of a respective society and espouse disadvantaged or extremist points of view. For the most part, these sites are anticoalition and try to drive a wedge between legitimate local police or military forces and the international coalition supporting these forces.

Insurgents have used the Internet to cyber-mobilize primarily in two ways. First, the Internet is used 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 commit. Second, the Internet is used to post influential information items to include jihadi training materials, an ideological rationale for actions, instructional manuals, propaganda, and agitation materials online. Some creative methods have been used. For example, a recent posting to a jihadi Web page announced a competition to design a new Web site for an Iraqi militant group. The motivating prize was the chance to fire missiles by remote control at a U.S. military base.[24] Insurgent Web sites have created, to some degree, a paperless environment in which insurgents can operate.

Other cyber-age developments are also of tremendous value to an insurgent. For example, the CD is one such device. CDs, with messages from suicide bombers (or more likely with just extremist songs or music), have been found in places as far apart as Riyadh, Saudi Arabia, and Lansing, Michigan. Thus it is not always necessary for potential Middle East recruits to possess a computer or Internet connection to obtain insurgent propaganda—just access to some device that plays a CD. Insurgents are also using some traditional forms of PSYOP. For example, in April 2006, insurgents in Iraq firebombed several bookstores, news kiosks, and distribution points and scattered leaflets that read, "All who associate with these newspapers will be the legitimate target of the mujahideen wherever they are, and the mujahideen will not waver in targeting them and killing them."[25] Further, insurgents use many other old propaganda techniques. They distort facts and sequences of events, they place blame on the innocent, they make comparisons that are favorable only to them, and they berate their enemies. The difference between old uses of propaganda and new uses, of course, is that the Internet can quickly spread insurgent claims around the world with speed, clarity, and efficiency. In some regions of the world, even the wildest insurgent claims are accepted at face value.

U.S. Terminology: Does It Neglect the Virtual Insurgency Aspect of Conflict?

The terms insurgency and insurgent are used throughout this chapter, but each term carries with it a traditional utilization that has no virtual association. This is clear from both formal and informal explanations of the terms. It is important for planners to develop and elucidate virtual insurgency terminology, as the cyber world begins to influence operations and summon insurgents to the front much like radio transmissions once did.

Both U.S. President George Bush and former Defense Secretary Donald Rumsfeld shied away from the term insurgent and its virtual implications.

Rumsfeld, speaking at a press conference in 2005, said he was a little reluctant to call the people the coalition is fighting in Iraq "insurgents." He preferred the words "enemies of the legitimate Iraqi government."[26] In response, language expert William Safire noted that "insurgent, from the Latin *insurgere*, 'to rise up,' means 'a rebel, one who revolts against an established government.' The insurgent in rebellion does not have the status of a belligerent, rooted in Latin for 'waging war,' and thus does not have the protections in law of a member of a state at war."[27]

It appears that when Secretary Rumsfeld speaks of enemies of the legitimate government, he is indeed talking about an insurgent, since Safire's definition (which corresponds closely with the dictionary definition) is so similar (an insurgent is a rebel who revolts against an established government). One who revolts is often considered an enemy—or can turn into one when the "revolt," as in Iraq, lasts for a period of time and involves brutal slayings. Safire believes that Rumsfeld does not like the term insurgent for two reasons: it is often applied to a group seeking to oust the leadership of a political party or a union (acting much like an underdog and attaining the sympathies of the population), and it unifies disparate elements into an "insurgency."[28] These factors are cause for concern. For example, a Jihad Academy video showed operations carried out by the Mujahideen Army, the Islamic Army in Iraq, the Ansar al-Sunnah Army, and al Qaeda in the Land of the Two Rivers, indicating that several insurgent groups do exist and their unification could make them even more difficult to handle.

President Bush, in his 2005 commencement speeches at the Naval Academy and at Kansas State University, also avoided the term insurgent. He defined the coalition's enemy in Iraq as "a combination of rejectionists, Saddamists and terrorists." The president believes rejectionists are resentful Sunnis who can be brought into the Iraqi democratic folds, Saddamists are those wanting to return to power, and terrorists are foreigners fighting freedom's progress in Iraq, according to an explanation by Safire. By not lumping these three together into the term "insurgents," the president hopes to keep them from uniting in the minds of Iraqis (keep the violent factions separate from the rejectionists).[29] Again, no mention is made of the virtual arena in which these groups operate.

Joint Publication 1-02: *The U.S. Armed Forces Dictionary of Military and Associated Terms,* last updated in March 2006, defines an insurgency and an insurgent as follows:

- *Insurgency*: an organized movement aimed at the overthrow of a constituted government through use of subversion and armed conflict
- *Insurgent*: member of a political party who rebels against established leadership[30]

Again, as expected, there is no mention of a "virtual" insurgent. There would also appear to be a disconnect, however, between these definitions and others previously noted. In fact, the "official" *Joint Publication 1-02* descriptions can serve as a source of confusion. An insurgency, according to the *Joint Publication* definition, does not necessarily have to be an organized "political" movement, yet an insurgent is defined as one who is a member of a political party. This is odd and inconsistent. The definitions also do not conform to the *Webster's Dictionary* definition of the terms either. As with other terms[31], it is clear that more precision is needed in U.S. military terminology. Such imprecision may be the impetus that motivates presidents and defense secretaries to start interpreting the meaning of words, which generates further confusion in society and among the armed forces as to what or whom our forces are fighting.

British military expert John Mackinley, whose recent work has centered on a concept called "the virtual arena of war," sees a new type of insurgency emerging—one that neither President Bush nor Secretary Rumsfield nor *JP 1-02* have mentioned. According to Mackinley, "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.[32] A complex insurgency grows organically like a virus and acts intuitively. To defeat it may require reorganized security structures and an unfamiliar modus operandi."[33] The idea of a complex insurgency and the concept of organic growth much like a virus would complement nicely Secretary Rumsfield's fears that the disparate units could integrate forces intuitively and spread. One must be careful, however, 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 the palm of an insurgent as a cell phone at the tactical level.

Mackinlay adds that "the virtual dimension should not be confused with information warfare and must be regarded as an arena of activity that no single party controls; it is not, therefore, a special weapon exclusively in the hands of any particular user. Just as friendly and enemy forces act against each other in the strategic and operational spaces, so they do in the virtual dimension."[34] Mackinley believes that the virtual dimension's proliferation of actors has created another theater of war with key objectives and tactical areas that can be seized by either side, and that a counterstrategy must contain interconnected strategic, operational, and virtual dimensions.[35] This arena is turning PSYOP into CYOP, a cyber-enabled psychological mobilization and recruitment factor of which coalition defense planners must be aware.

Joint Publication 1-02 defines a counterinsurgency as "those military, paramilitary, political, economic, psychological and civic actions taken by a government to defeat insurgency. Also called COIN."[36] Once again, no virtual element is noted. The closest definition in *Joint Publication 1-02* to a counter cyber mobilization capability would be the term "cyber counterintelligence," which is defined as "measures to identify, penetrate, or neutralize foreign operations that use cyber means as the primary tradecraft methodology, as well as foreign intelligence service collection efforts that use traditional methods to gauge cyber capabilities and intentions."[37] This focus relates more to conventional computer network operations than it does to any mobilization activity. Overall, one is left with the feeling that the mobilization aspect of the insurgency and counterinsurgency doctrine has received short shrift and that IO has ignored the cyber element so prominent in civil society.

To counter the impact of these mobilizing Web sites and devices in theater, U.S. brigade commanders and other coalition leaders—in the absence of an adequate information operation "quick response" template (IO is one of the designated concepts to counter insurgent information actions)—have developed IO actions "on the fly." This fact alone indicates that something is at work in the cyber domain that current IO policy and strategy cannot address. Such actions are deemed more appropriate and conducive for the insurgency environment. Lieutenant General David Petraeus, former commander of the Combined Arms Center at Fort Leavenworth (and now the commanding officer of the troops in Iraq), noted at a recent IO conference that the key is speed.[38] Coalition forces need to respond to a situation by providing information to the population before the insurgents can act. While coalition forces admittedly did not receive much training (if any) on this issue in the past, the actual problem may lie elsewhere in the formulation of IO and the counterinsurgency doctrine.

Insurgents in Iraq and Afghanistan: How They Use Cyber Capabilities

Insurgents 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. Insurgents use the Internet to mobilize, recruit, manipulate, respond, and exploit modern conflicts faster than their opponents. Recently, Abu-Mus'ab al-Zarqawi, the former al Qaeda leader in Iraq, used the Internet to speak about U.S. 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. Meanwhile, the so-called Mujahideen Army posted a video titled "The Sniper of al-Fallujah." Such multimedia messages are often the persuasive and convincing element that influences the ideological or religious fence sitters to adopt their cause.

The Web facilitates the recruitment of suicide bombers from amongst these fence sitters. Terrorism researchers Scott Atran and Jessica Stern note that jihadist Web sites have played a key role in forging the mindset of a suicide bomber. The Internet provides a way to bond individuals and give them direction as they surf jihadi Web sites. Efforts are needed to provide a positive counter to them on the Internet, whether it be positive alternatives for those who might succumb to the recruiters or simply counters to these negative influences.[39]

Insurgent use of the cyber element has introduced an operating pattern different from a well-known U.S. military procedure, the OODA loop—a concept based on former U.S. pilot John Boyd's observe, orient, decide, and act paradigm. Boyd's paradigm determined a method for identifying and targeting an opposing force that worked well in the Cold War environment. Even while in flight there was time for Boyd to utilize all four elements. The paradigm works in Iraq or Afghanistan when coalition forces take the initiative, such as in the fight for Fallujah.

In Iraq and Afghanistan, however, it is often the invisible enemy that takes the initiative. Where (or who) they may be is often unknown. Insurgents hide and may initiate confrontation by remote control—as seen with IEDs—without ever confronting coalition forces. Only after an insurgent-generated incident does, or can, the coalition react. Coalition forces, given this scenario, cannot observe and orient—they must decide and act (or react). The invisible enemy has stolen the key elements of observation and orientation from them. Coalition forces must process the action that has taken place and coordinate it with policy before acting in many instances.

Insurgents use a different paradigm. A physical action occurs at their initiative and then they cyber-respond. The physical action, information response (PAIR) loop allows them to be the first to provide a version of a story to an audience with whom they have some credibility—one which offers them influence and support. The virtual dimension allows them to manipulate how an event is perceived before coalition forces can react.

U.S. Colonel Rob Baker, a former brigade commander in Iraq, recently provided a battlefield example of the PAIR paradigm by describing how an insurgent suicide bomber detonated his belt too early and killed a number of Iraqis, narrowly missing his intended target, a U.S. installation. Baker noted that it was vital for U.S. forces to immediately distribute suicide bomber or IED "handbills" that told Iraqis what had happened.[40] However, in this case, before information could be sent up the line to create the handbills, the insurgents beat U.S. forces to the information punch, spreading word that the U.S. had carried out a missile strike on the Iraqi populace (to cover up the insurgent's failed suicide mission). An anti-American crowd soon appeared, threatening to riot. Perhaps the crowd was not a result of an immediate Internet assemblage, but its actions would be reported there nonetheless. Meanwhile, our forces were properly running the incident through channels and awaiting word on what to do next. That is, the insurgents used the PAIR paradigm to perfection to gain advantage even from a failed operation.

Press reports indicate that 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 U.S. Federal Bureau of Investigation (FBI) noted that terrorist groups lack the ability to damage the United States via an Internet-based attack.[41] Thus the incredible force the United States has assembled to protect its information security is working well. But we have not done nearly as well at anticipating the insurgent's use of other cyber capabilities. A *Washington Post* article of August 9, 2005, described several ways in which the Internet can serve as a weapon for insurgents, such as:

- intertwine real-time war with electronic jihad,
- immortalize suicide bombers,
- taunt the U.S. military,
- release tactical details of operations many times each day,
- publish a monthly Internet magazine, and
- negotiate with bin Laden.[42]

By utilizing the Internet in this manner, the insurgents have become very effective, with a far smaller staff and effort than that which is employed by its coalition opponents. Jihadi Web sites 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 interested in attracting true believers to their cause as well as in convincing a broader audience of their political objectives.[43] Some insurgent audiences may not be as large as others, but they can be far more committed.

It is estimated that over the past five years, jihadi Web sites have increased from fewer than 20 to more than 4,000.[44] In this manner, the insurgency grows like a virus and acts intuitively. The Web sites enable insurgents to discuss their tradecraft and to exchange jihadist 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 jihadists, the Internet is not merely a place to publish open-source material; it is a place to conduct open-source war.[45] The Internet battle for influence and persuasion is second only to physical confrontation, some jihadists believe. A November 28, 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?[46]

A March 2005 statement on the jihadi forum Minbar Ahl al-Sunna wal-Jama'a noted that an Information Jihad Brigade had been formed—not an IO brigade, just an information brigade. The brigade's aim is to conduct a full-scale propaganda war to "influence the morale of our enemies." It is composed of design, language, and publication divisions. In December 2005, the Middle East Media Research Institute reported that insurgents are using Yahoo.com as a gateway for indoctrination and incitement of aspiring insurgents.[47] Perhaps this gateway is a product of the information brigade.

Web sites also allow jihadists to spread tactical and targeting information. An individual known as "al-Mohager al-Islami" ("The Islamic Immigrant") has been posting messages to dozens of jihadist e-group forums, both public and password protected, about the locations and equipment of U.S. and British sites in Kuwait, Qatar, and other areas. The 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 the mujahideen to target these sites. Thus, the Internet serves as an intelligence and reconnaissance asset for jihadists even in the planning stages of armed conflict. "Al-Mohager al-Islami" also provided a nearly 40-page pamphlet on "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 these crews to follow, observation points, kidnapping suggestions, and methods of capturing Americans."[48] On other Web sites, insurgents have actually placed warning orders to their subordinates when aware of future coalition activities. In one case, subordinates were warned to hide all papers and weapons because coalition troops would be searching their houses soon. Music and speeches can be uploaded on Web sites and forums as well.

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 January 23, 2006, video produced by the Global Islamic Media Front, entitled "Jihad

Academy," demonstrates this point more vividly. 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."[49] Once recruited, insurgents offer new recruits actual targets on the Internet against which action can be taken. For example, a review of Internet documents reveals a jihadist interest in targeting U.S. economic assets, especially oil installations or infrastructure in the United States.[50]

Insurgent use of the Internet for such targeting purposes represents a significant change in how warfare is perceived and understood, especially amongst the general population. One conclusion is that the Internet and associated Web sites, to put this in "army speak," may be the second most important insurgent force multiplier (improvised explosives remain number one). It enables insurgents to shape and influence local popular opinion and thereby manipulate the perceived outcome of coalition operations via the Web. No such resource was ever afforded insurgents in the past. Counterinsurgency plans to limit this capability will require extreme coalition sensitivity to local customs, values, and beliefs, as well as an understanding of both insurgent Internet operating procedures and methods to counter them.

American and Coalition Forces in Iraq and Afghanistan: How They Use Information Operations

As explained earlier in this chapter, the U.S. military would label most of these insurgent activities that involve the use of the Internet as "information operations"—an area of activity in which the military already has significant operational capacity and a strategic doctrine. Before U.S. forces entered Iraq in March 2003, they methodically prepared the proposed "information battlefield" based on nearly identical IO principles. This phase of the IO plan ended shortly after coalition forces arrived in Baghdad. Then a new phase of intensive IO planning ensued. Not unexpectedly, U.S. forces did not know completely what was being broadcast on the city's 15 radio stations, satellite TV networks, and the pages of newspapers that were still operating. The battle for Baghdad ended abruptly, and little planning, understandably, had been conducted for such an eventuality. It was more important to prepare for extended city fighting. Further, this was the first time our forces had encountered an information environment in an enemy city of this size. IO planners set about attacking this challenge, one that grew quickly once insurgent activities proliferated.

Army Captain Bill Putnam, a U.S. Army reservist who headed the coalition's Open Source Intelligence effort in Iraq for a period of time (which included the publication of the "Baghdad Mosquito," a document that reports on the latest street rumors in Baghdad), commented on this early effort. He noted that U.S. IO and the public affairs doctrine in Iraq were focused on making the Iraqi information environment conform to its doctrine. That is, the focus was on how things should be done (according to the doctrine), rather than allowing the environment to determine how IO should be conducted.[51] This is a huge problem according to Putnam, since he believes that "it is virtually impossible for a counterinsurgency campaign to be successful without some level of the local population's support."[52] Putnam therefore identified "how" the Iraqis receive information and formulate opinions as the most important issue for IO professionals to consider. Iraqis do so, he wrote, via satellite television channels, one's family and friends, the street (rumors), religious figures, and newspapers. It was this "circle of influence" that must be targeted if successful IO were to be conducted, Putnam believed. The IO template based on the doctrine did not correspond to the reality on the ground, a reality strongly influenced by cultural factors. But the U.S. armed forces have since responded aggressively to this oversight. Cultural factors are now an intense focus of armed forces time and planning, and IO strategy is showing renewed creativity.

At Fort Leavenworth's December 2005 IO conference, Colonel Baker confirmed the necessity of developing practical solutions to the IO challenges they faced and not relying solely on doctrine. He stated that intelligence and IO were the two most important aspects of the fight from his perspective. He felt it necessary to bypass the IO doctrine on several occasions and use his staff's creativity when the situation required. Baker noted that "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."[53]

Colonel Baker developed an "information battle rhythm" matrix that forced him and his staff to perform specific information-oriented events on specific days of the week (meetings with the media, local leaders, and so on). This matrix enabled him to not only keep his finger on the information pulse of the insurgency but integrate the local media and culture into his IO plan. He 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.[54]

There have been other coalition information successes in the war against the insurgents. For example, Iraqi state TV has publicized police hotline numbers for people to call to turn in potential or actual insurgents. There are also popular shows where captured insurgents confess to their crimes on TV under the tearful questioning or threats of those whose relatives the insurgent killed.

Thus, traditional IO ways of conducting 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 due to the situations they encountered. They were not focused on cyber mobilizing because they had all of the other resources (radio, TV, and news outlets) available to them in addition to the Internet. Perhaps this operating paradigm has inhibited our ability to get inside the insurgents' "cyber skin" and think or manipulate as they do.

As mentioned earlier, a major event involving our forces required a vetting process to understand what occurred before responding. This slow response mechanism is necessary, because it helps ensure that coalition forces aren't being manipulated by the insurgents. Too slow a response, however, gives insurgents time to develop a virtual force multiplier by providing the populous with a culturally astute version of an event modified to the insurgents' benefit. This enables a group of insurgent Web site designers and Internet responders to influence the population much to the same extent as the coalition's highly organized and financed IO effort. Coalition forces need to develop an insurgent-oriented "countercyber capability" for their IO lexicon and action portfolio. They need to get outside their IO think box and into the insurgent's cyber think box.

Learning from the Two Lawrences

Lessons learned from Iraq and Afghanistan are being spread amongst coalition forces, and they are adapting to the insurgent's operating environment. Those studying the cultural aspect often note that in order to better understand how to deal with insurgent behavior, one should read the work of T. E. Lawrence that describes his dealings with Arabs in the 1920s. The *London Times* on May 22, 2005, wrote that General John Abizaid, CENTCOM commander, quotes Lawrence on a regular basis. The cultural lesson most often cited from the work of T. E. Lawrence, it seems, is reflected in his oft-cited advice:

> Do not try to do too much with your own hands. Better the Arabs do it tolerably than that you do it perfectly. It is their war, and you are to help them, not to win it for them. Actually, also, under the very odd conditions of Arabia, your practical work will not be as good as, perhaps, you think it is.[55]

However, if the Internet, as stated earlier, "is the greatest weapon in the armory of the modern jihadist," then this is because the civilized world has provided jihadi commanders with both the infrastructure and means to run their "modern printing press." Meanwhile, modern armies appear unprepared to handle the consequences of this fact—that is, the development of a proper counterinsurgent or other suitable neutralizing capability. The topic of jihadist Internet usage was hardly mentioned at the December 2005 IO conference.

Insurgents are using the Internet more effectively than coalition forces due to their lack of moral or legal restrictions and due to the situational context (particularly the coalition presence in a Middle East country). Many disaffected Internet surfers believe what is written on jihadi Web sites and want to support their cause. Further, the irrational tenth tactic that Lawrence discussed (that tactic "not taught but ensured by instinct, sharpened by thought") also has an insurgent application. Their tactics are developed in a context void of laws and mercy but with a deep cultural and instinctive understanding of what their messages will mean (both factual and implied) to their audience. Coalition forces do not possess this instinct for connecting with the population. This insufficiency should embolden further cultural studies in the U.S. armed forces to develop a higher degree of proficiency in this area.

Another Lawrence whose sayings also have tremendous applicability to the current insurgency in Iraq and Afghanistan is an unlikely source—that being Lawrence "Yogi" Berra. Berra, a tremendous New York Yankee catcher in the 1950s and 1960s, is well known for his sayings of counterintuitive malaprop value. Of relevance here is his saying that "in theory, there is no difference between theory and practice. In practice, there is." That is, one can read about insurgencies and stability operations and IO, but one cannot foresee the context in which these operations are conducted or interpreted. One can read about IO, but its application in practice, as Colonel Baker pointed out, requires an entirely different type of thinking, one tied to the environment and the target set to be affected.

Coalition forces are finding this out as they confront insurgent forces that have access to an information means (the Internet) that enables them to cyber-plan, finance, recruit, mobilize, and exploit faster than their opponents in the virtual theater of war. They are able to exploit a cyber echo effect through a multitude of Web sites today and do so with one-tenth or less of the coalition's IO infrastructure. This is a key observation of which all coalition IO experts should take note.

CONCLUSION

Noted author Hans Magnus Enzenberger stated over a decade ago that the nature of war was changing from "purposive, ideologically driven enterprises undertaken by highly organized industrial powers" to "molecular civil war."[56] Insurgent tactics worldwide appear to fit Enzenberger's description.

The Internet offers a new spin, however, on Enzenberger's molecular civil war theory. Insurgents have gained an ideological and motivating force multiplier with the Internet, as it communicates insurgent-generated interpretations of events via images and messages. Insurgents are often more culturally attuned to the needs and desires of the local population than an occupying force and are able to adapt their messages to these sensitivities.

Coalition forces, on the other hand, have a limited frame of reference for understanding the world around them. They are not closely associated with the populations with whom they are interacting in many cases and thus have difficulty associating with cultural sensitivities as well as monitoring and analyzing the plethora of Web sites available to insurgents and their potential sympathizers. The Internet allows jihadists to produce a cacophony of culturally related responses (both messages and pictures) to actions they take or mistakes the coalition makes. Insurgents apply no ethical standards to their Internet use. They utilize hate propaganda and one-sided interpretation of events to generate support. Coalition forces must do as much as possible to counteract this capability. Demonstrating how insurgent Web sites differ in content based on their target language is an example of one counterpropaganda possibility. That is, coalition forces could translate serious disparities in content between Arabic and English sites back into the original Arabic for Iraqi domestic political consumption. This would allow them to see the two-sided linguistic game the insurgents are playing.

The civilian community offers some other optimistic developments. Recently, the Foundation for the Defense of Democracies, which purportedly includes Muslims, Christians, Jews, and secular organizations in its membership, started the "Coalition against Terrorist Media." Its Web site[57] has several interesting sections such as "What is Terrorist Media?" "Terrorist Media in the News," and "View Terrorist TV." Weimann offers other possible countermeasures in his study. These are some of the first steps toward the counterpropaganda mechanism that needs to be developed by coalition forces for contemporary and future conflicts.

Further, the civilized world must continue to closely watch the impact of jihadist propaganda on children, particularly in the Middle East, where poverty and alienation make the Internet messages more alluring. Children under the influence of this virtual arena of the insurgent's cognitive warfare, whether it be video games or Internet cartoons, could turn out to be tomorrow's IED specialists.

Coalition commanders recognize the fact that they 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, writing, "Counterinsurgency warfare is the realm of the officer who can think beyond the textbook, who thrives in the absence of rules."[58]

If Colonel Baker is correct, that intelligence and IO are the two most important aspects of the environment in Iraq and Afghanistan, then more attention must be paid to them. This probably requires a different IO tool or mindset than that currently available within the Department of Defense. U.S. IO specialists must study the Internet's use by insurgents and learn to focus on "how" the circle of influence works in a particular culture, what the images are that matter, and so on.[59] They must learn how to develop "countercyber" plans and actions and how to manage the consequences of these actions. As a result, both the elements of the IO doctrine and the term counterinsurgency as currently defined should be expanded. As noted above, counterinsurgency is officially defined as "those military, paramilitary, political, economic, psychological and civic actions taken by a government to defeat insurgency. Also called COIN." The definition should also add some form of the "cyber mobilization monitoring or destruction tool" concept. The IO list of core capabilities requires similar refinement.

Jihadi worldwide cyber mobilizing and recruiting activities do not stop at U.S. borders, according to the Web site of Laura Mansfield. Mansfield, who has appeared as a guest speaker on *CNN* with talk show host Anderson Cooper, notes that there is an emerging danger unfolding on the Web pages of MySpace, the social networking site for teenagers. Her analysis indicates that there are several sites on MySpace advocating jihadist activities,[60] which, if true, indicates that jihadist cyber activities are truly now in "our space." One of the functions that MySpace performs is to list the number of "friends" that a certain site attracts. These "friends" of jihadist sites on MySpace indicate that, while not of any particular danger at the present (some subscribers advocating jihadist activities list friends in the low hundreds), MySpace is developing as a potential local recruitment tool for insurgents.

The conclusion drawn from this discussion is that virtual elements are the agitators and propagandists of today's insurgency much like pamphlets, journals, and leaflets were at the time of the French Revolution. These virtual or cyber elements mobilize the population much like leaflets and pamphlets once did. However, the effect of the virtual arena is more effective in that it is incredibly responsive and dramatic, offering videos, testimonials, and other images often directly from the site of some significant operation. Cyber elements are immediately responsive to breaking news and are available 24/7.

The U.S. IO doctrine will have to take this fact into account, as will the counterinsurgency terminology and doctrine, if both want to stay engaged and productive in the information field. With warfare changing from armies massed against one another to high-tech local wars in which insurgents can play a primary role, the virtual arena becomes very important. Armies cannot stand between cyber-generated stories and the interpretations and fears of the local populace. Past insurgencies did not rely on the Internet's power to cybermobilize as do today's insurgencies.

Fine-tuning our IO counterinsurgency definitions and enhancing our understanding of cyber mobilization is required if we are to be more aware and adept at handling this emerging cyber challenge.

ACKNOWLEDGMENTS

The views expressed in this report are those of the author and do not necessarily represent the official policy or position of the Department of the Army, Department of Defense, or the U.S. government.

NOTES

1. "Most Foreign Fighters in Iraq Come from Egypt: U.S. Military," AFP, Yahoo News, June 30, 2006.

2. Katherine Shrader, "Pentagon Surfing Thousands of Jihad Sites," Associated Press, May 4, 2006, http://www.forbes.com.

3. It is hard, if not impossible, for Internet viewers to make distinctions among insurgent groups. All insurgent anticoalition propaganda sounds much the same. Neither the Internet source nor the Web creator's attributes are often known with certainty in the virtual arena of war.

4. Audrey Kurth Cronin, "Cyber-Mobilization: The New Levee en Masse," *Parameters* (Summer 2006): 77–87.

5. Ibid.

6. Ben Venske, "Evolution of Jihadi Video (EJV) V1.0," *Journal of Counterterrorism and Homeland Security International* 12, no. 1, 50–51.

7. Ibid., 50.

8. Injy El-Kashef, "Islam Dot Com," *Al-Ahram Weekly*, October 20, 2005.

9. T. E. Lawrence, "The Evolution of a Revolt," in *The Army Quarterly and Defense Journal* (October 1920): 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 March 1, 2006.

10. Gabriel Weimann, *Terror on the Internet* (U.S. Institute of Peace, 2006), 6–7.

11. Ibid., 30.

12. Ibid., 150.

13. Ibid.

14. The "correct" English spelling of the group's Arabic name is Hizb'Allah or Hizbu'llah; however, it is more usually spelled "Hizbollah," "Hizbullah," or "Hezbollah." In order to standardize across all three volumes, the editor has chosen "Hizbollah" because that is the spelling employed in the URL designating the group's official homepage.

15. The game is offered via its own Web site http://www.specialforce.net/english/indexeng.htm.

16. Ibid., 92.

17. Ibid., 91.

18. Albert Bandura, "Training for Terrorism through Selective Moral Disengagement," in *The Making of a Terrorist: Recruitment, Training and Root Causes*,

vol. 2, ed. James J. F. Forest (Westport, CT: Praeger Security International, 2005) 34–50; Also, see Albert Bandura, "Mechanisms of Moral Disengagement," in *Origins of Terrorism: Psychologies, Ideologies, Theologies, States of Mind,* ed. by Walter Reich (Cambridge: Cambridge University Press, 1990), 161–191.

19. Anthony Stahelski, "Terrorists are Made, not Born: Creating Terrorists Using Social Psychological Conditioning," *Journal of Homeland Security* (March, 2004), available online at http://www.homelandsecurity.org/journal/Articles/stahelski.html.

20. Marc Lynch, "Al-Qaeda's Media Strategy," *National Interest* (Spring 2006): 54.

21. *Joint Publication 3-13, Information Operations,* February 13, 2006, GL-9.

22. Jeff Crawley, "Proponent Hosts Info Ops Gathering," *The Lamp*, Fort Leavenworth, Kansas, December 22, 2005.

23. Neil Doyle, "Digital Gap Seen in War on Terror," *Washington Times,* February 18, 2006, as posted in the Information Operations Newsletter, vol. 6, no. 9, February 17–March 9, 2006, 13.

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

25. "Analysis: Insurgents Target Newspaper Vendors, Distributors," Open Source Center Internet Site, April 8, 2006.

26. William Safire, "Mideastisms," *New York Times Magazine*, January 15, 2006, 16.

27. Ibid.

28. Ibid.

29. Ibid.

30. *Joint Publication, JP 1-02, Department of Defense Dictionary of Military and Associated Terms*, April 12, 2001, 127, 264.

31. For example, consider the term information war or IW: *JP 1-02* does not define war, so how can it define IW? Similarly, the term asymmetric warfare is used worldwide today, but *JP 1-02* does not define it either.

32. John Mackinlay, "Defeating Complex Insurgency," The Royal United Services Institute, Whitehall Paper 64, 2005, xii.

33. Ibid., vi.

34. Mackinlay, "Defeating Complex Insurgency," 13.

35. Ibid.

36. *Joint Publication JP 1-02, Department of Defense Dictionary of Military and Associated Terms,* April 12, 2001, 137, as updated through March 20, 2006.

37. Ibid., 138.

38. Crawley, "Proponent Hosts Info Ops Gathering," 1.

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

40. Crawley, "Proponent Hosts Info Ops Gathering."

41. ZDNet News, December 7, 2005, http://news.zdnet.com. U.S. 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 http://sfgate.com/cgi-bin/article.cgi, January 15, 2006.

42. Susan B. Glasser and Steve Coll, "The Web as Weapon," *Washington Post*, August 9, 2005, downloaded from the Internet (October 28, 2005).

43. For example, several insurgencies—such as the Tamil Tigers in Sri Lanka—offer several Web sites in different languages, reflecting what they believe will appeal most to particular targeted audiences. Thus, the Tamil version of their Web site is radically different from their Hindu or English versions in the images and words used to portray their group and the means by which they seek to achieve their political objectives.

44. For example, see Gabriel Weimann, "Terrorist Dot Com: Using the Internet for Terrorist Recruitment and Mobilization," in *The Making of a Terrorist: Recruitment, Training and Root Causes*, vol. 1, ed. James J. F. Forest (Westport, CT: Praeger Security International, 2005), 53–65; See also Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, DC: USIP Press, 2006).

45. Term used by John Robb to describe the insurgent's use of the Internet.

46. Stephen Ulph, "The Global Jihad's Internet Front," *Terrorism Focus* 2, no. 23 (The Jamestown Foundation, December 13, 2005).

47. "Terrorists Using Yahoo.com," WorldNetDaily.com, posted December 6, 2005.

48. SITE Institute, December 22, 2005, 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

49. www.jaami.com/vb/showthread.php, downloaded from the FBIS Web site and reviewed on January 25, 2006.

50. Stephen Ulph, "Internet Mujahideen Intensify Research on U.S. Economic Targets," *Terrorism Focus* 3, no. 2 (Jamestown Foundation), http://www.Jamestown.org.

51. Bill Putnam, "Winning Iraqi Hearts and Minds," *Army* (January 2005): 7.

52. Ibid., 8.

53. Crawley, "Proponent Hosts Info Ops Gathering."

54. Author's understanding of Colonel Baker's operational concept at the December IO conference.

55. T. E. Lawrence, from Wikiquote, downloaded from http://en.wikiquote.org/wiki/Thomas_Edward_Lawrence.

56. Hans Magnus Enzenberger, *Civil Wars: From LA to Bosnia* (New York: New Press), 1994.

57. See http://www.stopterroristmedia.org.

58. Ralph Peters, "No Silver Bullets," *Armed Forces Journal* (January 2006): 39.

59. For a description and analysis of the most common jihadi images, please see the report "The Islamic Imagery Project," published by the Combating Terrorism Center at West Point, available online at http://ctc.usma.edu/imagery.asp.

60. See http://blog.lauramansfield.com/2006/05/18/teen-terror-on-the-web-jihadi-and-islamist-activities.htm