Of Shoes and Sites: Globalization and Insurgency

Captain Christopher M. Ford, U.S. Army, J.D.

IN 1965, two years before his execution at the hands of Bolivian counterinsurgent troops, Ernesto Rafael "Che" Guevara, the famed South American Marxist insurgent and guerrilla fighter, found himself deep in the African jungles of the Congo passing along advice similar to that found in his book *On Guerrilla Warfare*: "The vital necessities of the guerrillas are to maintain their arms in good condition, to capture ammunition, and, above everything else, to have adequate shoes."[1]

Guevara had been dispatched from Cuba to assist the Marxist Simba insurgency against the government of Mobutu Sese Seko.[2] His Congolese acolytes must have presented a conventional picture of an insurgency: a group of scruffy, ideological men huddled in secrecy around a charismatic leader, learning the ancient art of guerrilla warfare.

Guevara's instruction traded on insurgents of the past, most notably Mao Tse-tung, and focused on the principles of rural insurgency, a form of warfare distinguished by small cells of insurgents exploiting their knowledge of the terrain and their ability to operate independently with few organizational needs—save functional arms and, of course, good shoes.[3]

At roughly the same time, in another jungle across the globe, the United States was busily engaged in its distinct brand of counterinsurgent operations—Operation Rolling Thunder, the bombing campaign of North Vietnam. During the course of the campaign, which lasted until late 1968, the U.S. Air Force flew 306,380 bombing sorties.[4] By all accounts the operation was a failure, and quite possibly the model for how not to fight an insurgency.[5]

Today, 42 years later, the United States is again fighting a robust insurgency. The intervening four decades, however, have wrought a worldwide change in technology, information, mobility, culture, and warfare. These changes, collectively defined as "globalization," have touched virtually every aspect of human conduct, counterinsurgency warfare included.[6] Thus, the picture of the modern counterinsurgent is that of a soldier on the streets of Baghdad, dressed in an Advanced Combat Uniform, protected by ceramic body armor, communicating with a satellite phone, and armed with an M-4 carbine and a fistful of reconstruction dollars.

What Is Insurgency?

In examining insurgency and globalization, two questions become readily apparent: (1) What is insurgency and (2) What aspects of globalization are pertinent to the discussion? We can define an insurgency as "an organized

Captain Christopher M. Ford, U.S. Army, is an assistant professor in the Department of Law, United States Military Academy, West Point. He holds a J.D. from the University of South Carolina and a B.A. in political science from Furman University. His assignments, in part, include a tour in Baghdad, Iraq, as the command judge advocate for the 5th BCT, 1st Cavalry Division, and as the operational law attorney for the 1st Cavalry Division.

PHOTO: This image, downloaded from the Internet on 3 March 2005, shows the front cover of an online magazine purportedly posted by Al-Qaeda's affiliate in Iraq, launching an effort to recruit Muslims to join its campaign to drive the United States and its allies from Iraq. The magazine is named Zurwat al-Sanam, Arabic for "The Tip of the Camel's Hump"—a reference among Islamic militants to "the epitome of belief and virtuous activity." (AP Photo)

movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict."[7] Insurgency movements traditionally find their roots in a desire for social and/or political change, and then insurgencies utilize guerrilla warfare to accomplish their goals.[8] This distinction between insurgencies and insurgency movements is important because counterinsurgent operations are more expansive than counterguerrilla operations—the latter term refers exclusively to the engagement of the insurgency's military force. In this article, "counterinsurgency" refers to full-spectrum operations designed to target the insurgency politically, economically, and militarily.

Successful insurgencies have certain fundamental prerequisites. Field Manual (FM) 31-20-3, *Foreign Internal Defense Tactics, Techniques, and Procedures for Special Forces,* summarizes these as a vulnerable population, strong leadership, and lack of government control.[9] The most basic requirement is the positive support or at least the acquiescence of the population. As noted by Mao Tse-tung, "Because guerrilla warfare basically derives from the masses and is supported by them, it can neither exist nor flourish if it separates itself from their sympathies and co-operation."[10] A vulnerable population, electrifying leaders, and a government's failure to control movement allow insurgencies to garner popular support more efficiently and effectively.

An insurgency must maintain popular support throughout its course, and actually increase it during its later stages. At the outset, the insurgents need support to move a radical idea, discussion, or plan from something conceptual to something tangible—to a physical (usually military) manifestation of the movement. The movement continues to require support as the government mobilizes to defend its position of power and monopoly on the use of force within the country. As the insurgency matures, it will likely progress from guerrilla to conventional warfare as it seeks to destroy (rather than harass or injure) the national power and establish ever-larger territorial bases of operation.[11] As this occurs, violence increases, and the insurgency must justify the violence as necessary to attain objectives the people will support: more security, more prosperity, a more just national power, and so forth.

The insurgency gains, maintains, and grows its popular support by communication, not only through the media, but by physically treating civilians with respect. Numerous insurgent writings fully discuss this second theme, which has not changed in the face of globalization.[12] Oral and written communication through the media, however, has everything to do with globalization. Insurgencies communicate internally from leader to leader, leader to fighter, and fighter to fighter, and externally to civilians and the international community.[13] At the outset, insurgencies have to rely on secrecy to prevent the annihilation of their defenseless fledging organization; however, their need to communicate remains high. The proliferation of technology has largely solved this problem.

Mobile Phones and Insurgency

Globalization includes a broad range of changes that affect insurgent operations, but the most profound change is the globalization of technology.[14] The mobile phone has been at the forefront of the technological charge.[15] Since the mid-1980s, mobile-phone use throughout the world has increased at breakneck speed.[16] At present, 80 percent of the world's population has mobile-phone coverage, and 25 percent has a mobile phone.[17] The medium's benefits to the insurgent are obvious: it provides a remarkably effective, easy-to-use, largely anonymous global communications network at virtually no cost.[18]

Mobile phones do, however, present a number of problems for insurgencies. Previous insurgencies relied on personal communications from insurgent-to-insurgent and insurgent-to-civilian and tightly controlled the dissemination of information, which served both their ideological and security interests. With the advent of mobile phones, insurgent leaders' ability to control the dissemination of essential information (i.e., ideology, strategy, etc.) has become more difficult. Mobile-phone use has also exposed the insurgent to the counterinsurgent's technological superiority.[19] It is widely accepted that both the Irish Republican Army and Al-Qaeda largely abandoned mobile telecommunications because they felt they were vulnerable to counterinsurgent monitoring.[20]

Mobile phones have also affected the counterinsurgent, though not to the same degree. As early as May 2003, the Coalition Provisional Authority (CPA) in Iraq was working to build a mobile-phone network in Iraq. The CPA sought to "establish

U.S. Army, SGT Tierney P. Nowland

U.S. Army SFC Daniel Ogawa and an interpreter examine a suspicious cell phone found outside a house in Mansour, Iraq, 4 April 2007, during a combined cordon and search mission with Iraqi Army soldiers.

wireless service," a laudable goal for a counterinsurgent organization.[21] Studies show that a rise in the use of mobile phones results in an increase in the gross domestic product, which, in turn, fosters faith in the government and helps quell insurgency.[22] Presumably, the CPA had a perhaps more pressing desire to establish a telecommunications network for its organizational use. Since the establishment of mobile-phone networks in Iraq in 2003, the U.S. Departments of State and Defense have utilized these networks extensively for official business. Indeed, 95 percent of U.S. military communications occurs over commercial phone lines.[23]

This technology, however, comes with a price. Because counterinsurgent soldiers and civilians connected with the military might be able to purchase phones for their personal use (as ours do in Iraq), the counterinsurgent can face the same security issues the insurgent faces. Insurgents can easily monitor unsecured counterinsurgent mobile-phone conversations through readily available police scanners, or they can physically tap secure and unsecured phone lines strung out building-to-building in the camps and forward operating bases of the counterinsurgency.[24]

The Internet and Insurgency

Fortuitously for the insurgents, technology provided a solution to their operational security problem through a combination of two other paradigm-shifting technologies: the Internet and user-friendly "strong-encryption." The Internet, in particular, has profoundly enhanced insurgent communications, operations, and organization.

Impact on communication. The Internet's most obvious and perhaps most profound impact has been in the realm of communication. Insurgents can select from a menu of communication choices, including e-mail, instant messaging, chat rooms, websites, blogs, Voice over Internet Protocol, and related technologies, and use them as their needs arise. While Internet communications present the same OPSEC issues as mobile/satellite phone networks, their diversity and multiplicity of means constitute an ever-expanding cyber-universe that the counterinsurgent must monitor.

The counterinsurgent is further hobbled by the proliferation of strong-encryption software freely available on the Internet since the release of Pretty Good Privacy (PGP) 1.0 in 1991.[25] This software revolutionized secure communications by using complex encryption algorithms in a simplified manner accessible to the average computer user. The result: arguably unbreakable electronic communications. This technology continues to increase in strength with the release of newer programs and versions (e.g., there have been at least eight new versions of PGP). Now, the technology is being adapted to provide the same level of security for voice communications.[26]

The Internet also allows an insurgency to appeal to a broad swath of people both inside and outside the targeted country. Through the Internet and the associated spread of information, globalization has broadened the insurgency's ability to propagate its message to consumers who previously would never have had access to it. Insurgent (and terrorist) organizations have quickly embraced the Internet and mobile phones to disseminate propaganda, recruit

The Internet…has profoundly enhanced insurgent communications, operations, and organization.

fighters, and solicit arms and financial support.[27] Geography and the ability to physically print and disseminate literature no longer limit insurgencies. An organization such as Hamas may find a receptive audience in a living room in Middle America as well as in a fundamentalist madrasah in the Middle East.[28]

Impact on operations. In addition to extended communications reach, the Internet provides the insurgent a fully distinct plane of operation that transcends the traditional battlefield. We do not realize the full ramifications of this yet, and an in-depth discussion is beyond the scope of this paper; however, it is clear that insurgencies have proven adept at recognizing and adopting these new technologies. Computer hackers working for or sympathetic with insurgent movements from Serbia, Indonesia, and Mexico have attacked or defaced dozens of corporate and government websites.[29] Other hackers have created computer viruses to support insurgent movements or to propagate a political agenda in locations as diverse as India, Iran, Hungary, England, Bolivia, Pakistan, Sri Lanka, Palestine, and the United States.[30]

Insurgencies always seek to become more operationally effective by executing their goals more efficiently while avoiding capture, injury, or death. An insurgency's ability to maintain or increase operational efficiency in the face of counterinsurgency operations demands that the insurgency constantly seek information in order to learn, adapt, and develop.[31] The acquisition of information has both transitory and enduring components.

Transitory information. At any given instant, incoming information provides the insurgency immediately beneficial consequences. Particularized, tactical application characterizes such information. (For example, an insurgent learns that counterinsurgent troops are preparing to raid a safe house, or an insurgent procures a map showing current troop positions.) Not surprisingly, with its myriad news sites, military-interest sites, and military-related blogs, the Internet is a rich source of information.

Globalsecurity.org, for instance, provides an extraordinarily broad and deep picture of counterinsurgent forces in Iraq.[32] The website posts descriptions and locations of individual camps and forward operating bases, troop levels, accounts of ongoing combat operations, and detailed analysis of current weapons systems. Most critically, it offers high-resolution satellite imagery of coalition troop positions. For instance, a series of images shows the "before" and "after" status of currently occupied coalition bases, including imagery of unhardened sleeping trailers. Google Earth, the satellite mapping service, offers similar information, and for that reason it has been publicly protested against by India, Thailand, and South Korea.[33]

Insurgents also reap current tactical information from the proliferation of Internet information on the manufacture of improvised explosive devices (IED). Traditional books providing the same information are readily available via websites such as Amazon.com, a cursory review of which found the following books for sale: FM 31-210, *Improvised Munitions Handbook*; FM 5-25, *Explosives and Demolitions*; *Expedient Homemade Firearms*; and *The Chemistry of Powder and Explosives*.[34]

Enduring information. The enduring aspects of information acquisition relate to the insurgency as an organization and its ability to acquire "new knowledge or technology that it then uses to make better strategic decisions, [to] improve its ability to develop and apply specific tactics, and [to] increase its chances of success in its operations."[35] As RAND Corporation's Brian A. Jackson notes, organizational learning is a four-part process involving acquisition, interpretation, distribution, and storage.[36] Globalization has facilitated each part of this process:

- The Internet provides a rich source for the *acquisition* of tactical information. As each piece of tactical information is acquired, interpreted, distributed, and stored, it becomes a building block for insurgency learning and growth.
- The Internet provides other information that is a core component of the learn/grow process, although not readily actionable: self-analysis, that is, counterinsurgent self-analysis, which aids and abets insurgent *interpretation* of gleaned information. In the case of most Western militaries, the Internet contains virtually countless internal government products analyzing all echelons and branches of service.[37] The interpretation of a particular piece of information is necessarily a highly individualized process; however, news stories, political commentary, interviews with soldiers and commanders, and poll numbers often facilitate this process.

- The third part of the organizational learning process requires *dissemination* of information. Dissemination of information is, of course, communication of information, a task, as noted above, immeasurably simplified by technology.
- The final step in the process involves the *storage* of information. This step ensures accumulation of a long-term institutional memory, allowing the movement to grow organizationally. Here, technology's globalization brought about a revolution in the conduct of insurgency. Where the organizational memory once resided in a handful of senior leaders and physical documents, a globalized insurgency may find its institutional memory committed to the Internet, where it is physically accessible but virtually indestructible. In the past, insurgent leaders possessed two unique qualities: they had the ability and authority to command and control, and they were the repository of the movement's institutional knowledge. Technology has rendered both qualities somewhat less than unique.

Impact on organization. The Internet's effect on insurgency organization and composition is related to, but distinct from, its effects on communications and operations. The dispersal of information technologies has given today's insurgencies a counterintuitive windfall. While it has diluted their leaders' ability to control information, thereby diluting the leaders' authority and power, its overall effect on the insurgency is positive.[38] Individual leaders no longer hold a monopoly on information disbursement and retention, but their groups have become hydra-headed entities with little or no hierarchical organization and a correspondingly diminished vulnerability. John Arquilla and David Ronfeldt have coined the term "netwar" to describe the method of warfare resulting from this organizational change. It is one "in which the protagonists use . . . network forms of organization, doctrine, strategy, and communication."[39] Because such an organization has no center of gravity, it presents a formidable problem for the counterinsurgent.

A 2004 RAND study documented the emergence of this phenomenon in Iraq. The study found "no clear leader (or leadership); no attempt to seize and actually hold territory; and no single, defined, or unifying ideology."[40] The present situation in Iraq, however, presents a somewhat different scenario. Elements of the insurgency have physically controlled, or sought to control, various geographic locales, including Najaf, Karbala, Ramadi, Sadr City, and Falluja. Further, the disparate elements of the insurgency do indeed appear to have adopted a unifying ideology, or at least purpose: they want to create insecurity in the population in order to force the occupation forces out. What the insurgency has failed to present, however, is a unified leadership. While elements of the insurgency appear to have leaders and a hierarchy (Muqtada al-Sadr, Izzat Ibrahim al-Douri, and Abu Hamza al-Muhajer most notably), the entire insurgency appears to lack a unified leadership and associated hierarchical organization.

So what do we make of all this? Iraq seems to present a hybrid insurgency, one containing elements of traditional insurgency along with the concepts embodied in netwar. Alternatively, one could argue that the situation in Iraq reflects a multitude of independent insurgencies, each developing individually in the classical form. What pattern the insurgency "fits" is a function of the amount of communication and coordination between its disparate elements—a source of perpetual debate. Under either model of insurgency, eliminating one element (senior leaders included) presents the counterinsurgent with yet another micro-insurgency or knowledgeable insurgent. The insurgent has fully dispersed his command, control, and intelligence. The counterinsurgent can never target the insurgency exclusively with tactical force.

Today's Global Battlefield

Earlier, we asked whom globalization advantaged and how it changed insurgency and counterinsurgency. The answers are now reasonably clear.

…a globalized insurgency may find its institutional memory committed to the Internet, where it is physically accessible but virtually indestructible.

Globalization has bestowed advantages on the insurgent. It has dispersed technology from the counterinsurgent nation-state powers so completely that it (technology) is now pervasive and even invasive, to the point where it influences all aspects of all conflicts. Plainly, since the insurgent now enjoys what the counterinsurgent has long had, the balance of benefits weighs heavily in favor of the insurgent. One intuitively recognizes that the new "globalized" insurgent has gained command, control, and intelligence benefits. Less intuitive, however, is globalization's impact on the insurgency's organizational structure, but globalization has perhaps most benefited the insurgency in this regard too.

…the new "globalized" insurgent has gained command, control, and intelligence benefits.

A globalized insurgency is a diffuse network of fighters and leaders communicating, learning, and executing through many indestructible technological outlets. Viewed in this manner, insurgency presents a substantial problem for the counterinsurgent. However, globalization encompasses the spread and integration of all aspects of the global community, to include ideas, markets, and information. Just as the counterinsurgent cannot prevent the spread of technology, the insurgent cannot prevent the spread of ideas, markets, and information to civilians caught in an insurgency. The counterinsurgent must disrupt and minimize the insurgent's use of technology while dominating and bolstering the population's access to ideas, markets, and information.

The mechanism for this is perhaps best illustrated through a passage in the book *The Lexus and the Olive Tree*, wherein Thomas Friedman quotes Nobel laureate Murray Gell-Mann on the issue of complex systems: "With a complex non-linear system you have to break it up into pieces and then study each aspect, and then study the very strong interaction between them all. Only this way can you describe the whole system."[41]

In other words, the counterinsurgent must understand the conflict's components and the relationship between them. The components are civilians, counterinsurgent forces, insurgent forces, and the world community. The counterinsurgent must resist imposing a meta-structure over the insurgency or attempting to identify a single leader. Identifying a single high-value target to kill, such as Musab al-Zarqawi, sets the counterinsurgent a difficult goal whose accomplishment requires prodigious resources that may produce only modest benefits.

An insurgency is fueled by communication, not only within the insurgency, but perhaps more important, communication from the insurgency to the civilian population. Thus, success for both the insurgent and counterinsurgent rests with the civilian population. As FM 3-07, *Stability Operations and Support Operations,* notes, "Success in counterinsurgency goes to the party that achieves the greater popular support."[42] Insurgents rely on a supportive (or at least neutral) population to facilitate their movement and operations. The counterinsurgent tries to induce the population to turn against the insurgency and to reject its use of force to dispense justice. Both sides seek to carry their viewpoint through physical acts and by propagating information. Physical acts take the form of combat operations, raids, and IED attacks. Nonlethal physical acts include providing safety, reconstructing infrastructure, establishing a functioning judiciary, and providing medical care.

The counterinsurgent can disrupt the insurgency's propagation of information by lethally targeting the communicators and technologically disrupting the communication. The insurgent's message to the civilian population is, perhaps, the most important element of his communications. The counterinsurgent can dilute the insurgent's message through increased security, successful reconstruction projects, and respectful and controlled operations. He can influence the information the civilian population receives by using news releases, signage demonstrating reconstruction successes, television and radio broadcasts, personal leader engagements, and such controversial actions as giving away satellite dishes, providing free Internet service, overtly and covertly favoring beneficial local news coverage, and blocking detrimental media broadcasts.

Technology has assisted the insurgent by enhancing his ability to disseminate information and to

survive and adapt so that the communication of the message can be continued. Disrupting the insurgent's advantage is a function of understanding the nature and organizational structure of the globalized insurgency, focusing efforts on targeting the civilian population with information, and continuing combat operations against insurgent cells.

Globalization has enabled the distribution of a multitude of ideas and technologies, and in doing so it has, to some extent, empowered the insurgent. Nevertheless, if the counterinsurgent secures and facilitates the marketplace of ideas, insurgent violence and disorder will eventually give way to accord and prosperity. ***MR***

NOTES

1. Ernesto Rafael Guevara de la Serna, *On Guerrilla Warfare* (New York: Praeger, 1961).

2. Robert B. Edgerton, *The Troubled Heart of Africa: A History of the Congo* (New York: St. Martin's Press, 2002), 205.

3. Fleet Marine Force (FMF) Reference Publication 12-18, trans. Samuel B. Griffith, *Mao Tse-tung, On Guerrilla Warfare* (reprinted 5 April 1989 [originally published in 1961]).

4. John T. Correll, "Rolling Thunder," *Air Force Magazine* 3 (March 2005).

5. Ibid. ("The campaign's failure is beyond dispute.") See also Colonel John K. Ellsworth, *Operation Rolling Thunder: Strategic Implications of Airpower Doctrine*, United States Army War College (AWC), Carlisle, PA, 4 June 2003.

6. See, generally, Thomas Friedman, *The Lexus and the Olive Tree* (New York: Straus and Giroux, 1999), and LTC Antulio J. Echevarria II, *Globalization and the Nature of War* (Carlisle, PA: AWC, Strategic Studies Institute, March 2003). For a fascinating and ever-engaging debate on the nature of the current revolution in military affairs, see, for example, John Arquilla and David Ronfeldt, eds. *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: The RAND Corporation: 1997); Thomas X. Hammes, *The Sling and The Stone: On War in the 21st Century* (St. Paul, MN: Zenith, 2004); Antulio J. Echevarria II, *Fourth-Generation War and Other Myths* (Carlisle, PA: AWC, Strategic Studies Institute, November 2005); John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar, and Information-Age Terrorism," in Ian O. Lesser et al., *Countering the New Terrorism* (Santa Monica, CA: The RAND Corporation, 1999).

7. Department of Defense Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: U.S. Government Printing Office [GPO], 12 April 2001), 264.

8. U.S. Army Field Manual (FM) 90-8*, Counterguerilla Operations* (Washington, DC: GPO, 29 August 1986), 4-7, defines guerilla warfare as actions "causing disruption, confusion, and harassment. These actions may be conducted by conventional or unconventional forces."

9. FM 31-20-3, *Foreign Internal Defense Tactics, Techniques, and Procedures for Special Forces* (Washington, DC: GPO, 20 September 1994), 3-4. See also FM (Interim) 3-07.22, *Counterinsurgency Operations*, (Washington, DC: GPO, 1 October 2004), 1-1 through 1-8.

10. FMF Reference Publication 12-18.

11. Mao Tse-tung most famously described this progression of insurgency. FM 90-8, FM 3-07.22, and FM 3-07, *Stability Operations and Support Operations* (Washington, DC: GPO, February 2003) adopt a similar framework.

12. Mao Tse-tung, "Be Concerned With the Wellbeing of the Masses, Pay Attention to the Methods of Work" (speech made to the Second National Congress of Workers and Peasants, January 1934); Ernesto Guevara, *Guerrilla Warfare* (Lincoln: University of Nebraska Press).

13. Joel J. Clark, "The Effect of Information Technologies on Insurgency Conflict: Framing Future Analysis*" (*masters thesis, Naval Postgraduate School, Monterey, CA, 1998), 6-7.

14. In an early, seminal work on the topic, John Mackinlay broadly organizes the effects of globalization on insurgency into five categories: transport technology, communications, deregulation of the international economy, migration, and culture. See John Mackinlay, *Globalization and Insurgency* (New York: Oxford University Press, 2002).

15. As used in this article, the term "mobile phone" includes satellite phones.

16. See, for example, "Semi-Annual Data Survey Results: A Comprehensive Report from Cellular Telecommunications and Internet Association (CTIA) Analyzing the U.S. Wireless Industry," CTIA—The Wireless Association, June 2005, a report showing a 955 percent increase in mobile-phone usage from June 1985 to June 2005; "The World in 2006," *The Economist*, 102, notes that India is adding 2.5 million new mobile-phone subscribers each month.

17. "Motorola to Offer Ultra Low-Cost Phones: Sub-$40 Models Aimed at Emerging Markets," 14 February 2005, MSNBC, <www.msnbc.msn.com/id/6448213/did/6969423>.

18. As mobile-phone use has proliferated, the cost of the technology has deceased proportionally. Thirty U.S. dollars is the current price point for an entry-level phone. The global telecommunications companies anticipate this figure to decrease to $15 by 2008. See Dan Nystedt, "Mobile Industry Focuses on Handsets for the Poor," 30 September 2005, <www.infoworld.com>.

19. The National Security Agency's ECHELON program is a prime example. Niall McKay, "Lawmakers Raise Questions About International Spy Network," *New York Times*, 27 May 1999.

20. MAJ Kevin C. Leahy, "The Impact of Technology on the Command, Control, and Organizational Structure of Insurgent Group" (thesis, U.S. Army Command and General Staff College, Ft. Leavenworth, KS, 2005).

21. Coalition Provisional Authority website, <www.iraqcoalitiona.org/ES/comms.htm>.

22. A recent study by London Business School found a direct correlation between mobile-phone usage and gross domestic product. "New Research Examines the Link Between Mobile Phones and Economic Growth in the Developing World," *The Economist*, 12 March 2005, 94.

23. Bruce Berkowitz, "Warfare in the Information Age," *Issues in Science and Technology*, Fall 1995, 59-66.

24. A cursory review of the Internet found a number of sites providing easy instructions on monitoring mobile phones. See, for example, <www.snapshield.com/www_problems/Inter/All_you.htm>.

25. See <www.pgp.com/company/history.html>.

26. Phil Zimmerman, the creator of Pretty Good Privacy, is developing a programmed codenamed zFone that would allow users to encrypt VOIP conversations. See <www.philzimmermann.com/EN/zfone/index.html>.

27. Terrorist organizations in particular have fully embraced the Internet to propagate their ideas. For a comprehensive discussion of this, see Minji Daniels, "Online Islamic Organizations and Measuring Web Effectiveness" (masters thesis, Naval Postgraduate School, Monterey, CA, 2004); LTC Patrick S. Tibbetts, "Terrorist Use of the Internet and Related Information Technologies," unpublished paper, School of Advanced Military Studies, Fort Leavenworth, KS, 2001.

28. For an example, see the English-language pro-Hamas website at <www.palestine-info.co.uk/am/publish/ liberties_0.shtml>.

29. Hackers sympathetic to the Zapatista movement in Mexico used a program called FloodNet to disrupt U.S. and Mexican corporate sites; another hacker defaced the websites of Mexico's finance and heath ministries; Serb hackers defaced NATO's website; and hackers supporting an autonomous East Timor defaced dozens of Indonesian websites. John Arquilla and David Ronfeldt, *Swarming & The Future of Conflict* (Santa Monica, CA: The RAND Corporation, 2000), 2; The Hacktivist.com, <http://thehacktivist.com/hacktivism.php>.

30. "Son of Zafi Email Worm Attacks Hungarian Prime Minister, Sophos Reports on Virus with a Political Agenda," 28 October 2004, <www.sophos.com>.

31. Brian A. Jackson, et. al., *Aptitude for Destruction: Volume 1: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism* (Santa Monica, CA: The RAND Corporation, 2005). This article provides a fascinating, comprehensive analysis of how terrorist organizations learn.

32. <www.globalsecurity.org>.

33. Katie Hafner and Saritha Rai, "Google Offers a Bird's-Eye View, and Some Governments Tremble," *New York Times*, 20 December 2005, A1.

34. See <www.amazon.com/exec/obidos/ASIN/1881801012/rightocom/002-9726936-6888044>.

35. Ibid.

36. Brian A. Jackson, et al., 10-14.

37. See <www.globalsecurity.org/military/ops/oif-lessons-learned.htm>. Further, the AWC Strategic Studies Institute, the Air War College, the National War College all provide extensive current analysis conducted by senior leaders and military researchers. The U.S. Agency for International Development provides weekly updates on progress in Iraq. The Department of State periodically provides in-depth information regarding reconstruction progress, including contracts awarded, power generation numbers, oil production numbers, and reconstruction dollars spent.

38. For a dissenting opinion, see Anthony Vinci, "The 'Problems of Mobilization' and the Analysis of Armed Groups," *Parameters* (Spring 2006): 56-58. Vinci argues that an insurgency needs some level of leadership.

39. John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: The RAND Corporation, 1996), 5.

40. Bruce Hoffman, *Insurgency and Counterinsurgency in Iraq* (Santa Monica, CA: The RAND Corporation, 2004), 16 (citations omitted).

41. Thomas Friedman, *The Lexus and the Olive Tree* (New York: Farrar, Straus and Giroux, 1999), 24.

42. FM 3-07, 3-4.