Fighting Back: New Media and Military Operations

By

Dennis M. Murphy

Fighting Back: New Media and Military Operations

By

Dennis M. Murphy

Executive Agent:
Center for Strategic Leadership, United States Army War College

Published: November 2008

U.S. ARMY WAR COLLEGE
CARLISLE BARRACKS, PENNSYLVANIA 17013

About the Author

Dennis M. Murphy is a Professor of Information Operations and Information in Warfare at the U.S. Army War College. Professor Murphy served in a variety of command and staff positions over his 27 years of U.S. Army service to include command of a direct support artillery battalion forward deployed to Germany and an associate professorship at West Point. Professor Murphy was appointed as the first George C. Marshall Fellow for Political-Military and Diplomatic Gaming at the Department of State's Foreign Service Institute in 1999. His work in information operations (IO) and strategic communication includes a tour as senior observer-trainer for the Battle Command Training Program, Operations Group Delta (Joint Task Force and Combatant Command trainers) where he trained NATO multinational forces on IO prior their initial deployment to Bosnia. He has written on information operations, strategic communication and national security issues and published in Military Review, Field Artillery Journal, Foreign Service Journal, NECWORKS Journal, and Parameters among others. His most recent article, "The Trouble with Strategic Communication(s)" appears in the winter 2008 issue of IO Sphere. Professor Murphy currently serves as the Director of the Information in Warfare Group at Center for Strategic Leadership, U.S. Army War College where he teaches information operations and strategic communication elective courses and conducts workshops focused on the information element of power.

Introduction

The Israeli-Hezbollah War of 2006 provides recent, glaring evidence of how the current information environment has impacted the way warfare is conducted today. Hezbollah masterfully manipulated and controlled that environment to its advantage, using (at times staged and altered) photographs and videos to garner regional and worldwide support.[1] If this doesn't sound new, it shouldn't... especially if you are an Israeli. Hamas effectively used the same techniques to turn the Battle of Jenin in April, 2002 into not only a strategic informational victory, but a historical legend of resistance that lives on today in the hearts and minds of Palestinians. The Israelis, having won total tactical victory in Jenin, literally snatched defeat from the jaws of victory by abrogating the information battlespace to Hamas.[2] Certainly, United States military leaders can, at a minimum, empathize with the Israelis. Insurgent use of information as an asymmetric strategic means has been extremely effective in the current theaters of Iraq and Afghanistan leading Richard Holbrooke to famously muse: "How can a man in a cave out-communicate the world's leading communications society?"[3] Had Holbrooke even superficially studied recent history he could have answered his own question. The monopoly enjoyed by nation-states over information as an element of power was rapidly lost as technology improved and as the means to transmit that information became smaller, faster, cheaper and, consequently, ubiquitous. And the outlook in that regard certainly does not seem to favor lumbering bureaucracies any time in the future.

These enabling technological capabilities have popularly been tagged "new media." Broadly, new media has been described as "that combustible mix of 24/7 cable news, call-in radio and television programs, Internet bloggers and online websites, cell phones and iPods."[4] But, of course this menu limits the definition to present day capabilities and is quickly outdated given current and expected future technological advances. New media in this context quickly becomes "old" media, especially in light of projected asymptotic increases in speed and capacity. So, a more timeless definition should consider new media as any capability that empowers a broad range of actors (individuals through nation-states) to create and disseminate near-real time or real time information with the ability to affect a broad (regional or worldwide) audience.

If the United States military hopes to fight and win in a future information environment dominated by new media it must fully understand both the opportunities and challenges of that environment. This includes the ability to exploit new media to achieve military objectives and defeat an adversary's skilled

use of it within real and perceived bureaucratic and legal constraints. A review of these capabilities and their use reveals a requirement for a significant cultural shift within the military, while recognizing that current planning processes remain valid. It also points to the importance of competing on the information battlespace, not only in counterinsurgency operations, but across the spectrum of conflict.

New Media and Today's Information Environment

The current information environment has leveled the playing field for not only nation states, but non-state actors, multinational corporations and even individuals to affect strategic outcomes with minimal information infrastructure and little capital expenditure. Anyone with a camera cell phone and personal digital device with internet capability understands this. On the other hand, the United States military has increasingly leveraged advances in information infrastructure and technology to gain advantages on the modern battlefield. One example from Operation Iraqi Freedom is the significant increase in situational awareness from network centric operations that enabled coalition forces to swiftly defeat Iraqi forces in major combat operations.[5] Another includes the more prevalent use of visual information to record operations in order to proactively tell an accurate story or effectively refute enemy "dis-information."

Even a cursory look at advances in technology confirms what most people recognize as a result of their daily routine. The ability to access, collect, and transmit information is clearly decentralized to the lowest level (the individual). The technology is increasingly smaller, faster and cheaper. Consequently, the ability to control and verify information is much more limited than in the recent past. Nor will it get any easier.

> *In 1965, the physical chemist Gordon Moore, co-founder of Intel, predicted that the number of transistors on an integrated chip would double every eighteen months. Moore predicted that this trend would continue for the foreseeable future. Moore and most other experts expect Moore's Law to remain valid for at least another two decades.*[6]

So, if you're into control, as nation-states, bureaucracies and the military tend to be, the future may appear bleak since not only is the ability to access, collect and transmit information decentralized, the capacity to do the same continues to increase exponentially. With this in mind consider both the new media capabilities and methods currently used and where the future may be heading as the basis for understanding what this means for the warfighter.

The Internet

The internet is the obvious start point for any discussion of the impact of new media. It is important to note that the World Wide Web, as a subset of the internet, is essentially ungoverned, providing obvious freedoms and cautions. The web gives the individual a voice, often an anonymous voice…and a potentially vast audience. Websites are easily established, dismantled and reestablished, making them valuable to extremist movements. Islamic extremist websites grew from twenty to over 4,000 in only five years.[7]

Web logs (blogs) are another example of the power that the internet provides to individuals along with the dilemma they pose for nation-states. There were 35.3 million blogs as of April 2006 reflecting a doubling of size every six months of the previous three years.[8] Most of these, of course, have little effect on the conduct of nation-states or their militaries, but those that gain a following in the national security arena, can have a huge impact. President George W. Bush recently cited Iraqi bloggers to point to progress being made in Iraq,[9] having apparently learned both the importance and value of blogs in 2004 when investigative bloggers cleared his name in the infamous CBS airing that questioned his military service.[10] The U.S. Central Command actively engages dissident voices by participating in blogs that are critical of the war on terror noting "with the proliferation of information today, if you're not speaking to this forum, you're not being heard by it."[11]

Video use and dissemination has skyrocketed as the capabilities of the internet have increased. The YouTube phenomenon's power and access is evidenced by its purchase for $1.6 Billion by Google only 20 months after its founding. Like blogs, YouTube serves a variety of purposes to include entertainment. But, also like blogs, YouTube can empower individuals to achieve strategic political and military effects where easy upload of their videos, without editorial oversight, allows access to a nearly unlimited audience. Thus, the use of the improvised explosive device (IED) by insurgents shifts from a military tactical weapon to a strategic information weapon when the IED detonator is accompanied by a videographer. And again, like blogs, the United States military has recognized the importance of competing in the video medium, using YouTube to show ongoing images of U.S. operations in Iraq.[12]

While websites, bloggers and video proliferate in today's internet ("web 2.0") the "over the horizon" technology of "web 3.0" while in its infancy, is rapidly increasing in popularity. Web 3.0 is generally about being inside a 3D virtual world that is low-cost and emotive. This is the "metaverse" or virtual universe of

applications like Second Life and others. Second Life is attractive as an opportunity to socialize where there is no need to compete and can be exploited as a tool for learning. Multinational corporations see a movement where they will plan and execute business plans in the 3D internet world.[13] But, like the other internet based applications, web 3.0 provides opportunities for darker undertakings. The virtual universes show initial signs of providing training grounds for terrorist organizations and anonymous locations for criminal money-laundering.[14]

Mobile Technologies

The internet clearly is part of the new media phenomenon, but the internet has not penetrated large areas of the world, especially in the poorest areas of underdeveloped countries. The cell phone, however, as a means of mobile technology, is increasingly available worldwide and deserves discussion as a potentially potent capability to affect national security and military issues; arguably even more so than the internet.

There are numerous examples of cell phone Short Message Service (SMS text) messaging shaping political campaigns by mobilizing and revolutionizing politics. It is used both to call people to popular protests as well as used by governments to provide misinformation in order to quell such protests. Text messaging is the medium of choice in overseas countries. It bypasses mass media and mobilizes an already persuaded populace as a means of lightweight engagement. Cell phones currently contain the technology to text, provide news, video, sound, voice, radio and internet. Mobile is pervasive in the third world. 97% of Tanzanians have access to mobile phones. Mobile coverage exists throughout Uganda. There are 100 million handsets in sub-Saharan Africa. Radio is the only media device more prevalent than mobile. Consider the economic implications of mobile technologies as well. 59% of mobile phones are in the developing world–over seven million mobile subscribers in Kenya alone. Efforts are under way to develop African specific mobile applications, e.g. distributing commodity prices (such as vegetable prices) to local village producers. Cell phones are used as credit cards in Kenya. You can pay for cab fare or for fish at the market with your cell phone. Cell towers are being raised in Lake Victoria to allow fisherman to call to shore with their catch numbers as they set out to market. Mobile phones are ubiquitous in Asia. There are over 400 million users in China. Farmers receive crop market prices from the Chinese government via text messaging in order to allow them to harvest at the best possible time.15

Like any other new media capability cell phone technology provides opportunities and challenges. Many young Iranians are turning to cell phones as a means for political protest...an opportunity that can be exploited.[16] On the other hand, criminals and terrorists can use cell phones to quickly organize an operation, execute it and disperse using phone cards to provide cover from being traced. On an international scale, the challenge is often in the same laws that provide individual protections in democratic societies. Witness recent court battles within the United States regarding eavesdropping on foreign conversations without a court order when those conversations may be routed through a U.S. cell phone service provider.[17]

Mainstream Media in the Age of New Media

Mainstream media certainly takes advantage of technological advances in order to remain competitive. Marvin Kalb, in the Harvard report on the Israeli-Hezbollah War notes that:

> *To do their jobs, journalists employed both the camera and the computer, and, with the help of portable satellite dishes and video phones "streamed" or broadcast their reports..., as they covered the movement of troops and the rocketing of villages—often, (unintentionally, one assumes) revealing sensitive information to the enemy. Once upon a time, such information was the stuff of military intelligence acquired with considerable effort and risk; now it has become the stuff of everyday journalism. The camera and the computer have become weapons of war.*[18]

This real time reporting from the field has obvious impacts on the warfighter, but competition with new media for the first and fastest story also means that today's mainstream media is not your father's mainstream media. Because of the plethora of information available today, newspapers, which once competed for knowledge as a scarce resource, today compete for a new scarce resource: the readers' (or listeners' in the case of broadcast media) attention.[19] Perhaps that is why increasing numbers of young adults turn to Jon Stewart's "The Daily Show" for their news.[20] It should come as no great shock, then, that "good news" stories about military operations do not appear with regularity in mainstream print and broadcast journalism.[21] Good news doesn't sell...because it doesn't grab the reader's (or viewer's) attention.

Of course in an environment where the speed of breaking news means viewership and thus advertising dollars, accuracy is sometimes sacrificed as well. In a strange twist, mainstream media now turns increasingly to bloggers

for their stories and the most respected bloggers require multiple sources to verify accuracy.[22] Consequently, the distinction between new and mainstream media sources becomes blurred, leaving it to the reader, already bombarded with information, to distinguish fact from fiction (or perhaps more accurately "spin" from context).

The U.S. Military: The Impact of New Media

The impact of new media in today's information environment has significant implications for the U.S. military. The first, and perhaps most obvious, is that individuals and small groups (e.g. the terrorist franchised cell) wield information as a strategic, asymmetric weapon by very effectively leveraging new media capabilities. The lack of any bureaucratic structure further enables individual empowerment by also allowing a nimbleness of response that is the antithesis of nation-state governments. Additionally, the lack of governance of the World Wide Web allows any statements or positions to be presented without regard to truth, context or ethical foundation.

Current military doctrine espouses information superiority as the solution to the numerous dilemmas posed by new media:

> *To succeed, it is necessary for US forces to gain and maintain information superiority. In Department of Defense (DOD) policy, information superiority is described as the operational advantage gained by the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.*[23]

But this clearly is an unachievable definition of success given the challenges of the current and future information environment in which military operations take place. Individuals, empowered by new media capabilities, and unencumbered by bureaucratic processes and moral/ethical standards will continue to wield information as power asymmetrically. "Wildcards" will routinely gain resonance in the information environment and once the information is out it may be extremely difficult to refute or explain it (e.g. Abu Ghraib photos or Osama bin Laden's taped messages). Simply consider how corrections are made in mainstream print media. The correction is typically buried deep in the publication while referring to an article that likely appeared on page one above the fold. The chances of the original reader stumbling upon the correction are obviously slim. This reflects the "genie in a bottle" syndrome of today's information environment—once information is out of the bottle trying to stuff it back in is very difficult.

The Case of Jenin

The Battle of Jenin provides a relevant case study in both the impact of "wildcards" using new media means and the strategic impact resulting from a military that does not proactively and effectively manage the information environment.

Israel embarked on a military campaign in the spring of 2002 to root out entrenched Hamas terrorists in the West Bank of the Palestinian occupied territories. The Jenin operation specifically targeted approximately 200 militants operating within the city and was deemed a tactical success. The militant's infrastructure was destroyed, and a number of insurgents were killed and arrested. At the conclusion of the campaign terrorists attacks within Israel dropped off in the near term. However, the operation proved a significant strategic failure. Reaching the outskirts of Jenin, Israeli Defense Forces (IDF) restricted the media from entering the city. Thus, the information battlespace was abrogated to the militants. Framed digital photos of homes being demolished by Israeli bulldozers while frantic families looked on were transmitted quickly, and quite effectively, to the press and soon hit the international wires.[24] Cell phones were the only means of communication to the city and so the press used uncollaborated cell phone interviews with Jenin residents to tell their stories. These interviews spoke of massacre within the city in emotive tone and content.[25] While later disproved, those claims caused an international withdrawal of support for Israel. Further, Jenin remains, to this day, a mythical symbol of Palestinian resistance and Israeli ruthlessness among Palestinians.

The lesson of Jenin is that the military may be able to dominate the information environment in a localized geographical area for a limited period of time but these wildcards, using new media capabilities, become that limiting factor. So, if information superiority is effectively unachievable and information dominance can only be partially achieved how can the U.S. military succeed in the information battlespace? The answer is that the military can, and should be expected to *manage* the information environment on their terms. This requires playing a proactive role in shaping that environment as well as establishing processes to respond to those unforeseen stories that make dominance so difficult. Clearly, managing the "message" while controlling the necessary new media "means" represent critical challenges to that effort.

Nor should one be lulled into believing that the exploitation of new media as a military and strategic enabler is limited to insurgency operations. While insurgents

use new media to affect perceptions, attitudes and beliefs (the cognitive dimension of the information environment) nation states most recently have acted to exploit dependence on new media (specifically the internet) in the physical dimension, revealing an important vulnerability. Russia was alleged to have taken down Estonian government, bank and newspaper websites in what may have been a cyber-attack test in May 2007[26] prior to their combined cyber and kinetic attack on Georgia in 2008. China's People's Liberation Army (PLA), the most obvious near peer military competitor to the United States, has gained notoriety recently by being implicated in taking down Pentagon internet capability in June 2007.[27] The Chinese are transforming from a mechanized force to an "informationized" force and have stated intentions to use information warfare "as a tool of war (or) as a way to achieve victory without war...."[28]

New media is now playing, and will continue to play an increasingly important role in how the United States conducts warfare. How the U.S. military effectively manages an environment dominated by new media, therefore, becomes increasingly important to success in warfare.

Fighting Back: Managing the New Media Environment

The U.S. military has dealt with the new media phenomenon in fits and starts. Certainly one could argue that efforts to deal in this environment have largely been reactive rather than proactive. Soldiers using new media in the form of emails, blogs and digital photography revealed vulnerabilities of U.S. systems as well as operational tactics, techniques and procedures from current operations in Iraq and Afghanistan. This led to a top-down reemphasis on operations security, a program that has always existed, but never in the instantaneous world of information exchange, pointing again to both the power and danger of new media capabilities.[29] The YouTube and blog response efforts outlined previously are encouraging, albeit reactive efforts to manage this environment. One area of new media the military proactively exploits is knowledge management in order to share lessons learned from recent operational experiences. Interestingly, this process was bottom-up driven in the form of a web site independently developed by junior officers known as CompanyCommand.com. While the power in this forum admittedly lies in the dynamics of people and conversations, its potential would not be realized without the global and instantaneous reach provided by the internet.[30]

Reactive responses, however, will never allow the military to manage the information environment of today, nor the increasingly complex information

environment of the future. Instead, a proactive approach to fighting in that environment is necessary. This requires a cultural shift in the military mindset but not a doctrinal change in the way military operations are planned. The military has muddied the waters somewhat in that regard. Recognizing the need to compete in the information battlespace they have grappled with the concept of "information operations" in doctrinal publications and applied the concept in current operations with mixed results. Most recently "strategic communication" has entered the military lexicon.[31] Unfortunately these concepts are widely misunderstood by warfighters and often applied as afterthoughts by senior commanders in attempts to fix problems. Consequently, they become inherently reactive and often ineffective.

Senior military leaders have grown up in a culture that emphasizes kinetic warfighting skills, both in planning and execution. In order to ease the cultural transition from this world of bombs and bullets to one where information, driven by new media capabilities, is a significant weapon, it is best to work within both the language and planning methodologies inherent in that military cultural upbringing. Consequently, warfighters should consider and emphasize the "information effects" they wish to achieve in an operation. This focuses efforts on achieving a military objective, something commanders fully understand, and ensures the full range of capabilities available will be used to that end. The clear statement that will drive planners and subordinate units in that regard is the commander's intent.

The Commander's Intent, as part of the formal military planning process "articulate(s) the purpose of the campaign being conducted and the…commander's vision of the military end state when military operations are concluded."[32] It serves as the impetus for operational planning. The key to proactively managing the information environment, then, lies in a clearly stated *information* endstate, that is, a description of what the information environment will look like at the end of the military operation. The information endstate should consider both the cognitive and physical dimensions of the information environment. The cognitive endstate includes the desired perceptions and attitudes of the target audience (e.g. the indigenous population or international community). The physical information endstate includes a description of the new media capabilities of the adversary at the conclusion of the operation.

A properly articulated information endstate will drive both planning and execution of the military operation with sensitivity toward the new media environment. Military courses of action will be analyzed against this vision and

subordinate military units will carry out the operation in order to meet the endstate described within the intent. Sensitized to the commander' intent, planners "wargame" the courses of action with that endstate in mind. Consequently, the planners will consider an enemy's expected reaction to a friendly action in terms of the required information endstate. This will include recognition that a friendly kinetic action could result in an enemy asymmetric information reaction. Planners can then prepare for a counteraction to blunt the enemy information attack or choose an alternate course of action. Additionally, the information endstate will drive *how* subordinate units carry out their mission. Actions send loud and clear messages to a target audience. Where previously a kinetic solution may have been the preferred choice (driven by inherent organizational culture) the information endstate may instead drive the unit toward a different approach that achieves the stated cognitive effect on perceptions, attitudes and behaviors. The commander is now unburdened by unfamiliar concepts like information operations and strategic communication. To be sure, his planners and staff experts will apply those concepts to achieve the required information effect, but the key is that they will proactively do so. Nor will they limit themselves to information operations and strategic communication capabilities, but will use every available military capability available, in integrated fashion, to achieve the effect in support of accomplishing the military objective.

The information environment of today guarantees that "wildcards" will present themselves as unpredictable, disruptive forces to current operations. These incidents can significantly impact a military operation, whether the wildcard is the release of Abu Ghraib imagery...or terrorist internet video of gruesome beheadings. While the military response to such circumstances seems necessarily responsive in nature, current planning processes allow proactive consideration of such events as well. In military planning a "branch" is "a contingency option built into the basic plan.... It is used to aid success of the operation based on anticipated events, opportunities, or disruptions caused by enemy actions and reactions. It answers the question 'what if...?'"[33] Like the commander's intent, however, it requires an organizational culture shift in focus to apply the existing process to the expected new media information environment...but the widely understood process does exist. While branch planning cannot account for every possible wildcard (thus the name) it should anticipate that wildcards will occur and, at a minimum, establish procedures to deal with them.

The Battle of Jenin serves as an example of what could have been if IDF organizational culture had prescribed that the information environment be

addressed within the planning process. If the IDF Commander's Intent had articulated an endstate that addressed the cognitive dimension of the information environment would the battle have still resulted in strategic failure? Consider the effect of a stated military endstate where the people of Jenin would "remain neutral in their attitudes toward Israel" and "the international community would understand and support IDF efforts to defeat terrorism." Given that simple statement that drives planning and execution it is likely that the media would have been allowed to embed with the IDF during the battle in order to allow Israel to compete for international legitimacy. It's also likely that subordinate units would have carried out operations by using tactics other than bulldozing buildings to achieve their objectives in order to maintain Palestinian neutrality. Finally, branches to consider wildcards could have been developed that defined a process to address the now expected mis- and dis-information that the numerous cell phone interviews coming out of the refugee camps engendered. Those counter-wildcard procedures could have required IDF forces to carry helmet cameras to film operations to prove proportional response by the IDF and to immediately counter any framed or altered imagery distributed by the insurgents.

Given the importance of new media and the information environment, a statement of the information endstate must be required within commander's intent. This simple change in doctrinal requirement, supported by the military education system can drive organizational culture change and ensure the military proactively manages the information environment.

Conclusion

There is a generation gap between senior warfighters and their junior officers...a gap defined by digital immigrants and digital natives. The junior officers who developed CompanyCommand.com, as digital natives, fully appreciate the importance and power of new media and proactively exploit its capabilities. Senior warfighters, on the other hand, certainly understand its importance but lack the cultural upbringing to see it in the context of current military operations. Consequently, military operations are often impacted by unanticipated consequences enabled by the use of new media in today's information environment. Closing this gap to achieve success requires a cultural shift in the minds of these senior leaders. Introducing new concepts, like information operations and strategic communication, while academically interesting and militarily prudent, does not enable the required cultural enlightenment. Instead, as "new" concepts they lie outside the generational culture of these seniors who then often relegate the

information fight to specialized staffs established to understand those espoused doctrines and capabilities.

Recent proclamations by senior military leaders are encouraging regarding closing this generational gap. However, if the United States military hopes to fight and win in a future information environment dominated by new media then that gap must be closed as quickly as possible. Leveraging new media to achieve military objectives and defeat an adversary's skilled use of it requires a significant cultural shift at these senior ranks, but also recognizes that current planning processes remain valid. As Torie Clarke, former Pentagon press spokesperson, noted regarding information and its impact: "It comes down to people, planning and integration."[34] Implementing change within that construct is the easiest way to effectively impact a culture where managing the information environment is not only achievable, but must be expected.

Endnotes

1. Sarah E. Kreps, "The 2006 Lebanon War: Lessons Learned," *Parameters*, 37 (Spring 2007), p. 80.

2. Deidre Collings and Rafal Rohozinski, "Shifting Fire: Information Effects in Counterinsurgency and Stability Operations," U.S. Army War College: Carlisle Barracks, PA, 2006, pp. B9-B10.

3. R.S. Zaharna, "American Public Diplomacy in the Arab and Muslim World: A Strategic Communication Analysis," American University: Washington, DC, November 2001, http://www.fpif.org/pdf/reports/communication.pdf (Accessed September 25, 2007), p. 2.

4. Marvin Kalb and Carol Saivetz, "The Israeli-Hezbollah War of 2006: The Media as a Weapon in Asymmetrical Conflict," *John F. Kennedy School of Government Research Working Papers Series*, February 2007, p. 33.

5. Jeffrey L. Groh and Dennis M. Murphy, "Landpower and Network Centric Operations: How Information in Today's Battlespace Can be Exploited," *NECWORKS Journal*, Issue 1, March 2006.

6. Kevin J. Cogan and Raymond G. Delucio, "Network Centric Warfare Case Study, Volume II," (Carlisle Barracks, PA: U.S. Army War College, 2006), p. 4.

7. Timothy L. Thomas, "Cyber Mobilization: A Growing Counterinsurgency Campaign," *IOSphere* (Summer 2006), p. 23.

8. James B. Kinniburgh and Dorothy E. Denning, "Blogs and Military Information Strategy," *IOSphere* (Summer 2006), p. 6.

9. Sheryl Gay Stolberg, "Troop Rise Aids Iraqis, Bush Says, Citing Bloggers," *New York Times*, March 29, 2007, p. 17.

10. Kinniburgh, p. 5.

11. William R. Levesque, "Blogs are CentCom's New Target," *St. Petersburg Times*, February 12, 2007, p. 1.

12. Carmen L. Gleason, "Coalition Servicemembers Reach out to America via YouTube," *American Forces Press Service*, March 14, 2007.

13. The author attended a conference on "new media" sponsored by the Open Source Center at the Meridian House in Washington, DC in April 2007. The referenced comments reflect panelists' presentations. IBM already has a presence in Second Life with over 7,000 associates meeting and conducting business there. The conference was held under Chatham House rules allowing free and open dialog while ensuring the anonymity of speakers.

14. Natalie O'Brien, "Virtual Terrorists," *The Australian*, July 31, 2007, http://www.theaustralian.news.com.au/story/0,25197,22161037-28737,00.html (Accessed September 25, 2007).

15. Meridian House Conference notes.

16. John Moody, "A 'Celler's' Market for Information in Iran," *FoxNews*, June 14, 2007, http://www.foxnews.com/story/0,2933,282456,00.html (Accessed September 25, 2007).

17. Richard Willing, "Growing Cell Phone Use a Problem for Spy Agencies," *USA Today*, August 2, 2007, p. 2.

18. Kalb, p. 4.

19. Phillip Meyer, "The Proper Role of the News Media in a Democratic Society," *Media, Profit, and Politics*, The Kent State University Press: Kent, OH, 2003, p. 12.

20. Page Kollock and Suzanne Presto, "US Youth Use High-Tech Media for Political Communication," *VOAnews.com*, November 16, 2005, http://www.voanews.com/english/archive/2005-11/2005-11-16-voa5.cfm (Accessed August 24, 2007).

21. J.D. Johannes, "How Al Qaeda is Winning Evan as it is Losing," *TCS Daily*, July 11, 2007. The author provides a statistical analysis using "gross rating points" to convey that 65% of coverage of the Iraqi war is pessimistic.

22. Roxie Merritt, Director of Internal Communications and New Media, Armed Forces Information Service, interview with the author, February 22, 2007.

23. Chairman of the Joint Chiefs of Staff, "Joint Publication 3-13, Information Operations," February 13, 2006, p. I-5.

24. Collings, pp. B-9-B-10.

25. "Israeli Military Kills at Least 100 in Jenin Refugee Camp," April 9, 2002, http://www.democracynow.org/article.pl?sid=03/04/07/0256202. This site provides a "Democracy Now" radio interview with Ameer Makhoul by cell phone from inside the Jenin refugee camp.

26. Anne Applebaum, "e-Stonia Under Attack," May 22, 2007, http://www.slate.com/id/2166716/ (Accessed September 4, 2007).

27. Demetri Sevastopulo and Richard McGregor, "Chinese Hacked into Pentagon Defence System," *Financial Times*, September 4, 2007, p. 1.

28. Timothy L. Thomas, *DragonBytes: Chinese Information War Theory and Practice*, Foreign Military Studies Office: Fort Leavenworth, KS, 2004, p. 136.

29. Thomas Claburn, "Army Chief of Staff Calls for More Oversight of Military Bloggers," *Information Week*, September 1, 2005, http://www.informationweek.com/story/showarticle.jhtml?articleid=170102708 (Accessed September 22, 2007).

30. Nancy M. Dixon, et. al., *Company Command, Unleashing the Power of the Army Profession*, Center for the Advancement of Leader Development and Organizational Learning: West Point, NY, 2005, p. vi. Interestingly CompanyCommand.com was brought under the .mil domain to allow free flowing dialog while attempting to provide operations security.

31. Department of Defense (DOD) Joint Publication 3-13 provides a doctrinal overview of military information operations. Strategic Communication, as a nascent concept, has no doctrinal underpinnings, but was addressed in the most recent DOD Quadrennial Defense Review.

32. "Campaign Planning Primer," Department of Military Strategy, Planning and Operations, U.S. Army War College: Carlisle, PA, 2007, p. 13.

33. Chairman of the Joint Chiefs of Staff, "Joint Publication 5-0, Joint Operation Planning," December 26, 2006, p. IV-31.

34. Torie Clark, *Lipstick on a Pig: Winning in the No-Spin Era by Someone Who Knows the Game*, Free Press: New York, 2006, p. 172.