Marines at remote forward base enjoy rare opportunity to use social networking sites to communicate with family and friends

U.S. Marine Corps (Khoa Pelczar)

Mastering the Art of Wiki
Understanding Social Networking and National Security

By JAMES JAY CARAFANO

Computers, cell phones, other digital devices, and the systems that knit them together have altered how many on the planet do almost everything—especially how they share with each other. With over 1 billion people—some of them enemies of freedom—on the Internet, there is much more on the information superhighway these days than information.

There is a traffic jam of conversation facilitated by email, Facebook, LinkedIn, Twitter, and, of course, Wikipedia, as well as many other social networking tools (often collectively called Web 2.0) that facilitate discussion, debate, and the exchange of ideas on a global scale.[1] This unprecedented capacity to listen and respond is inexorably restructuring the ways that information is created and used. For example, during the 2008 U.S. Presidential election, the campaign of Barack Obama mobilized social networking in revolutionary ways to garner popular support and raise money, reaching a vast audience. The impact of social networking will not end with business and politics but will inevitably affect national security.

Social networking has the potential to touch every aspect of national security including gathering and vetting publicly available open source information, gauging and influencing public opinion, distributing "risk communications" (such as how to respond after a disaster), conducting research and analysis, developing policies, planning and implementing programs and activities in the field, and conducting information operations (the integrated employment of electronic warfare, computer network operations, psychological operations, deception, and operations security).

Dr. James Jay Carafano is Deputy Director of the Kathryn and Shelby Cullom Davis Institute for International Studies and Director of the Douglas and Sarah Allison Center for Foreign Policy Studies at the Heritage Foundation.

The Online World

There are basically two models for effectively distilling and sharing the best information in an organization—top down and bottom up. In the top-down framework, the senior leaders in an organization gather the best information. They use their wisdom, experience, and judgment to ensure that the information is shaped, edited, filtered, turned into knowledge, and then proliferated to the organization. Hierarchical knowledge creation and management work best in a static and predictable environment—one where senior leaders know best. In contrast, in

dynamic situations where experience counts for less, knowledge creation works best from the bottom up. At the grassroots, the immediacy of the junior leader turns out to be where the most effective learning takes place. Their experience is more fresh and relevant.

In the online world, the best knowledge comes from that bottom-up foundation, but that reality has problems as well as promise. Common wisdom holds that among social networks, the group itself assumes responsibility for culling out bad data. This includes everything from battling malicious actors online to pointing out simple errors—such as confusing pop star Michael Jackson with former deputy head of the Department of Homeland Security Michael Jackson. Wikipedia, for instance, is constantly keeping an eye on celebrity bio-pages to ensure that some star or head of state is not prematurely pronounced dead. Still, while the "rely on the crowd" method of adjudicating information may be suitable during normal social networking interactions, there is a real question over whether it is appropriate in matters touching on national security where lives and treasure may be at stake, where there is not time to let the network sort things out on its own, or where classified information once revealed cannot be put back in the safe.

The information jungle is a dangerous place. It has empowered both our scientific and narrative cultures. Information technology allows individuals to conduct more and better analysis, but it also allows opinion-makers to spin better, more compelling stories faster, and to proliferate them more widely. Digital-quick transparency can unmask evils or unearth secrets. Information that is massed to protect us can quickly be used against us. Secrets meant to be seen by almost no one can in minutes be leaked to everyone. The complacent may not survive long.

Information assurance cannot rely on the online crowd when national security is on the line. On such occasions, it is unrealistic to hold to the belief that negotiated Internet interactions are a sufficiently effective mechanism for determining factual and dependable information. Trusted actors and trusted networks must be established before crunch time, the terrible moment when lives and the fate of nations may be at risk. Trust and confidence are a must for a social network that can be depended on under stress.

Since the Internet is neutral, no party can count on a decisive and unassailable advantage across the "cyber-verse." For example, the debate over the impact of social networking on the Iranian election protests centered over whether these tools offered a clear advantage to the protestors or the government. Writing in the *Washington Post* in the wake of Tehran's post-election crisis, John Palfrey, Bruce Etling, and Robert Faris offered several counterpoints to those who had concluded that the force of online political activism is reversible. They argued that there are "sharp limits on what Twitter and other Web tools such as Facebook and blogs can do for citizens in authoritarian societies." Governments "jealous of their power can push back on cyberspace when they feel threatened." They also noted that the "freedom to scream" online may actually help regimes by providing a "political release valve." Repressive regimes can also employ social networking for their own ends, hawking propaganda and spreading disinformation.[2] Indeed, during the crisis, the Iranian government exploited all these advantages and in the end was able to largely stifle overt social unrest.

On the other hand, the Iranian government did not silence the voice of the people. Technology is continuously evolving, as are the practices of how the Internet is used. For instance, the regime in Tehran thought it could maintain permanent dominance of the Web by allowing only slow, expensive dial-up service. That assumption proved wrong. Social networking tools helped dissidents overcome the limitations of the nation's technological infrastructure.

There are also limits to what governments can do. If a regime such as Iran, for example, elected a "nuclear option" and tried to completely shut down the Internet to suppress internal dissent, it might well shut down its industrial, energy production, and financial sectors as well as crippling its capacity to control public media. Likewise, in a global economy, states or groups that conduct massive cyber attacks could do as much damage to themselves as to their enemy. Thus, a kind of "mutual assured destruction" deterrence appears to be evolving in the cyber world. At the same time, while some independent malicious actors may have no compunction about taking on a country, nations have every reason to seek to limit their ability to run amok. That, however, does not mean they will not try.

But nations have never been defenseless online, and even before America became super–security conscious after 9/11, the U.S. Government had not completely ignored post–Cold War threats to the Nation's peace and prosperity. Between 1998 and 2000, Congress held over 80 hearings on terrorism-related issues.[3] Efforts to enhance cybersecurity and combating malicious activity on the Web were on the list of things governments worried about. Likewise, there was a recognition that the Internet could serve as a tool of good governance. Efforts to make the Web serve people were undertaken as well. Instead of creating new practices and means of knowledge creation and knowledge management, E-Government was mostly about putting the way government already worked online. Even among governments, the United States was not the global leader. Nations such as New Zealand, Canada, and Singapore had more ambitious initiatives.

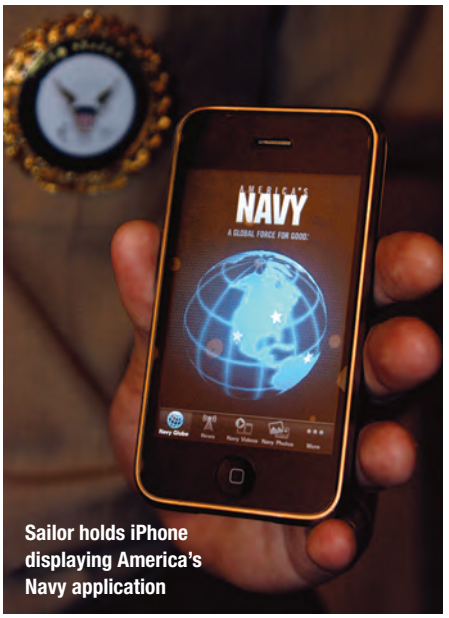
The "reality" of social network competition emerges again and again. It is wrong to look at cyberspace as a place for a static contest. There is no technology, government policy, law, treaty, or program that can stop the acceleration of competition in the cyber universe. Governments will not stop trying to rein things in, but it will always be a fight to the finish. No advantage will be permanent or unassailable. There will always be an enemy trying to take the cyber-heights.

Likewise, the platforms that carry network applications will likely change and evolve as well. Indeed, we are already seeing dramatic shifts in user preferences from personal computers to laptops to cloud computing to cell phones. Some, in fact, argue that computing is quickly becoming more a utility than a product. Software and hardware will mean less and less to social networkers as time progresses. Meanwhile, others are already predicting how online services will evolve, touting that Web 3.0 (where networks intuitively connect individuals to relevant information, not just other people) will soon supersede Web 2.0.

Still others look beyond and muse about the role of artificial intelligence in social networks. How we do what we do in social networks will likely continue to evolve, as will what we do with new applications. The bottom line is that it is a mistake to pin thinking about how social networks will work or what they will do in the future on any current platform or application. For now, what can be said of the global competition is that the two kinds of nations that are likely to be the most dominant competitors are those whose

U.S. Army (C. Todd Lopez)

Army is evaluating commercial handheld command and control solutions using Macintosh platforms



U.S. Navy (Michael B. Lavender)

Sailor holds iPhone displaying America's Navy application

regimes are the most authoritarian—and those whose societies are most free. Authoritarian regimes will utilize the brute force of control to seize social networking heights. Free societies will exploit the advantages of creativity, competition, and innovation. Both will prove remarkably resilient in online warfare. Both will be the main drivers in the course of the competition.

But the U.S. Government and, for that matter, many other governments are not well prepared to exploit social networking for national security. Bureaucracies often respond poorly to dynamic change and disruptive technologies. Web 2.0 can be both. There is growing unease that despite all the Washington talk of tackling cyber security and implementing cyber government, increasingly America may be "cyber-screwed." For starters, Washington is well behind in its willingness and capacity to adapt to the world of Web 2.0. Even President Obama, with his Blackberry by his side and a well-earned reputation as being Web savvy, has had his troubles. One of the first things the administration did in 2009 after moving into the White House was to revamp the President's Web site. A panel of experts assembled by the *Washington Post* gave the new WhiteHouse.gov site an average grade of C+.[4] That grade seemed to track well with the administration's response to the Iranian election protests. Even though there was a flood of information driving the global debate, as the protests grew, the President remained equivocal until several days into the crisis. Yet despite subdued rhetoric from the White House, the administration found itself pummeled by Iranian government accusations of interference, including a charge that an innocent bystander had been shot by the Central Intelligence Agency to foment a riot.

The disappointing results are not surprising. While the White House and many Federal agencies are experimenting with social networking tools, their efforts are largely unguided by sound research or clear and coherent policies that encourage innovation while protecting individual liberties and privacy. The hierarchical practices of traditional government are not keeping pace; they are inadequate for exploiting the explosion of social networking systems.[5]

There are a few lessons to remember when exploiting social networks, and for now we know what works. While there may not be hard and fast rules for social networking, there are some pretty good rules of thumb—principles for effective adoption of social networking tools that address the nature of the technology, structure of the social interaction, and value assigned to social networking transactions.[6]

The preference in social networking is to adopt proven and widely available software and systems that seem user friendly. Simple rules and simple operational routines are the hallmark of widespread adoption of social networking tools. The more intuitive the tool appears, the more likely it is to be adopted. And there has to be something in it for the user. Users are drawn to social networks because they believe participation will bring them a benefit they want. The recent proliferation of applications such as Web 2.0 Suicide Machine and Seppukoo (which allow users to purge their presence from online sites such as Facebook) reflects not so much a rejection of social networking as an affirmation that individuals are not terribly interested in a network from which they feel they derive no real value.

The Past Was Prologue

Government has had a hard time getting the "adapting" to technology part right from the onset of the information age. In 1996, the Clinger-Cohen Act placed major emphasis on information technology acquisition. It required Federal agencies to treat information technology as a "capital investment," hoping to get the government to think more strategically about all the hardware and software it was buying. The focus of the law, however, was on how agencies acquired new technologies rather than on what kinds of technologies and capabilities they were developing. Many government investments involved developing Intranets (private computer networks), standalone databases, and proprietary software. When the tsunami of social networking applications hit the market and open software offered a rich variety of tools for innovation and collaboration, the U.S. Government stood to the side saddled with a huge investment in systems and databases that operated independently from the Internet and one another. Government struggled to keep up with private sector technology, let alone try to network the public and private worlds.

During the Clinton administration, Vice President Al Gore gave a good deal of thought to defending the information superhighway. In Clinton's second term, policy guidance started to pour forth from the White House. On May 22, 1998, the administration published Presidential Decision Directives (PDDs) 62 and 63. PDD–62 highlighted the growing range of unconventional threats, including cyberterrorism, and initiatives for defending against them. PDD–63 focused specifically on protecting the Nation's critical infrastructure, which included the backbone of the World Wide Web telecommunications systems and the electrical grid, as well as significant users of online services such as the government, transportation, and financial sectors. Washington also spent a lot of time and money (about $100 billion) getting ready for "Y2K," an effort to ensure computer systems would not fail as a result of trying to account for dates in the year 2000.[7]

The combination of the Y2K scare, emergent fears over cyberterrorism, and growing dependence on the Internet led to the creation of the National Infrastructure Protection Center (NIPC), a joint government and private sector partnership that includes representatives from Federal, state, and local government agencies. NIPC tried to incorporate lessons learned from the Federal Government's Y2K efforts and threats of millennial attacks, launching a series of law enforcement and counterterrorism initiatives. In 2000, the White House formulated the first national cybersecurity strategy.

Networking would have been a natural solution for the public-private cooperation and information-sharing called for in the cyber crime report. Discussions of social networking, however, were noticeably absent in the report. Clinton and Gore may have been the first President and Vice President to exchange emails, but Web 2.0 was simply not on the White House radar screen. The Government's Terrorist Surveillance Program proved another intensely controversial initiative. The covert program, first revealed to the public in a December 16, 2005, article in the *New York Times*, authorized monitoring of every electronic social networking tool from telephones to the Internet, email, and text messaging. Since the surveillance might have included communications to U.S. Persons (a term that denotes American citizens and other persons legally resident in the United States), but did not require a search warrant, the program came under intense criticism. In response to the controversy, the Terrorist Surveillance Act of 2006 provided additional authority to conduct electronic surveillance and assigned the special Federal court established under the Foreign Intelligence Surveillance Act with the responsibility for issuing any required warrants for investigations.

Most of what became known about post-9/11 "offensive" efforts on the Internet became instantly controversial. On the other hand, the Intelligence Community's "defensive" capabilities were more mundane and less like lightning rods. In particular, strengthening cybersecurity was a key objective of the Information Sharing Environment (ISE) established in 2007. The ISE is a collection of policies, procedures, and technologies that permits the exchange of terrorism information, including intelligence and law enforcement data. It aims to promote a culture of data-sharing among its participants to ensure that information is readily available to support their missions. The ISE is supposed to connect Federal, state, local, and tribal governments. It also envisioned a critical role for private sector and foreign actors in sharing information to counter terrorist threats.[8] Even 3 years after it was called for, however, it remains—to put it kindly—a work in progress.[9]

In 1988, in response to a computer virus called the "Morris Worm," which was unleashed through the Internet by Massachusetts Institute of Technology student Robert Tappan Morris, Jr., and affected 10 percent of the Internet, the Government issued a contract with Carnegie Mellon University to set up a computer emergency response team (CERT), the first Federally funded team to respond to malicious outbreaks online. After 9/11, another Government initiative was the National Infrastructure Protection Plan (NIPP). Since most sectors of the economy utilize the Internet, cyber became a focal point of the NIPP, which relied on several institutions, particularly information-sharing and analysis centers, to facilitate the exchange of information with critical business sectors, such as financial institutions and energy companies. If the CERTs were the field soldiers of cyber response, the Information Sharing and Analysis Centers (ISACs) were the rear command posts. ISACs were established and funded by the private sector, with the data they handled largely provided by private sector participants. ISACs also receive information from other entities, including law enforcement agencies and security associations. In addition to the ISACs, critical business sectors have Sector Coordinating Councils that develop policy recommendations in coordination with government agencies.

In addition to the strategies outlined by Homeland Security in the NIPP, the Department of Justice kept a foot in the cyber war. Information-sharing between the Government and private sector receives considerable support from InfraGard, a program originally established by the Federal Bureau of Investigation under President Clinton. First developed to assist in cybercrime investigations, InfraGard expanded collaboration with law enforcement, business, and academia on a range of security-related issues after 9/11. InfraGard chapters facilitate information collection, analysis, and training and provide discussion forums to share best practices. It also provides a secure Web-based communications platform.

Private sector companies, universities, research centers, and nongovernmental organizations have also developed capabilities to combat malicious cyber activities and to investigate or disrupt terrorist operations on the Internet. Perhaps the best known of these groups is the Internet Security Alliance, a collaboration among the Electronic Industries Alliance, a federation of trade associations, and Carnegie Mellon University's CyLab, established to provide a forum for information-sharing and to generate suggestions for strengthening information security.

Many other organizations and private sector companies support America's cyber defenses. After 9/11, the U.S. Military Academy at West Point established a Combating Terrorism Center. It joined CompanyCommand and PlatoonLeader (both military networks) as innovative projects started by the academy to help "big Army" adjust to the new challenges of the online battlefield. Among the center's studies is the "Islamic Imagery Project: Visual Motifs in Jihadi Internet Propaganda," which provides a ready guide to commonly used terrorist graphics, symbols, icons, and photographs.

The University of Arizona has also conducted a multi-year project called Dark Web, which attempts to monitor how terrorists use the Internet. The university's Artificial Intelligence Lab has accumulated the world's most extensive database of terrorist-related Web sites—over 500 million pages of messages, images, and videos—and has made it available

to the U.S. military and Intelligence Community. Some of its sophisticated software exposes social linkages among radical groups and seeks to identify and track individual authors by analyzing their writing styles. The Middle East Media Research Institute (MEMRI) publicizes extremist messages on the Internet, including terrorist Web sites, discussion forums, and blogs. After MEMRI published a comprehensive survey of Islamist Web sites in 2004, many of them were closed down by their Internet service providers.

nongovernmental organizations and private companies provide a variety of analytical and investigative tools for penetrating terrorist operations on the Internet

In addition to these efforts, nongovernmental organizations and private companies provide a variety of analytical and investigative tools for penetrating terrorist operations on the Internet. For example, the Washington-based SITE Intelligence Group routinely monitors, translates, and posts information from terrorist Web sites and often shares that information with U.S. intelligence agencies.

Finally, software and hardware providers continue to respond to the needs of the marketplace with new services and products to counter illicit online activity, from combating unauthorized intrusions and countering denial-of-service attacks to preventing the disruption or exploitation of systems or data. Providing security services and products is a multibillion-dollar-a-year industry.

Befuddled Washington

Government social networking has an even greater challenge because it is not clear if Washington knows what it is trying to do online. This problem is nowhere more apparent than in government's effort to get its message out—a task usually called "public information" when the message is for American audiences and "public diplomacy" when communicating with the rest of the world. Struggling to get the message out and get it right is not new—particularly where matters of national security are concerned. In World War I, the policies promoted by George Creel, the head of the U.S. Committee on Public Information, tried to manage the global pandemic. Later American efforts wrangled equally inelegantly, attempting to promote and protect freedom and provide for free and open expression, all at the same time. Government officials have always had a hard time figuring out whether their job is to push out government's point of view or simply provide a forum for "objective" discussion. Public diplomacy and information programs during World War II were chaotic. Even America's vaunted efforts at combating the ideology of communism during the Cold War were marked by as many setbacks as successes.[10]

Richard Solomon, the head of the U.S. Institute of Peace, observed, "The opportunity is there for State to put out American perspectives on almost any issue, for anybody to pick up—the question is: What should the government be putting out?"[11] This is the same question public diplomacy has been asking since long before the Internet was invented. Washington still lacks a clear sense of purpose online and that is just as big a problem as grappling with the bureaucratic hurdles of exploiting new technologies. In mastering the struggle for the cyber high ground on both ends of the power curve, not knowing what you are trying to do is a real obstacle.

A big part of why Washington struggles is that it is just not good at problem-solving. The last quarter-century has seen an explosion in the human capacity to create and manipulate new knowledge. Despite that fact, the instruments used to inform public policy choices are as creaky as ever. Washington makes policy largely by intuition shaped by an orthodox adherence to 20th-century problem-solving—ideas that have barely evolved since the Cold War.

Even so, something dramatic has been added to the arsenal for analyzing today's challenges—the proliferation of computer technology, the Internet, and everything else that goes with the "information revolution." Modern researchers have access to vast digital libraries and databases as well as powerful search and computational programs. New means of manipulating data, such as *informatics* (the science of information processing), *data-mining* (extracting and analyzing data to identify patterns and relationships), *computer simulation* (modeling a system), and *open source intelligence* (acquiring and analyzing information from publicly available sources to produce actionable intelligence), to name a few, are delivering revolutionary instruments of knowledge discovery.

Ironically, knowledge discovery is proliferating in every field except national security. While the means of knowledge discovery have become more sophisticated, the process of public policymaking has become increasingly intuitive. In Washington, talking points, gut feelings, partisan preferences, and ideological fervor crowd out cutting-edge analysis. Building cyber-strategic leaders from this will be like building castles on sand unless the knowledge and skills imparted to them are based on comprehensive, practical, and unbiased research—research that specifically serves the needs of governments. Knowledge of the present is not good enough to be a first-class cyber competitor.

The debate over how great ideas can be created through Web 2.0 and what comes after it is far from over. Research in the field of social networking is hard pressed to keep up with the rapid pace of change in how information technologies are fielded and employed. Understanding social networking requires a multidisciplinary approach to research that combines the techniques of the social sciences with "hard science" disciplines. This mix of disciplines, which examines how networks function, is often called "network science."[12] Practitioners study diverse physical, informational, biological, cognitive, and social networks searching for common principles, algorithms, and tools that drive network behavior. The understanding of networks can be applied to a range of challenges from combating terrorist organizations to organizing disaster response. Without understanding, the science is all just guesswork and luck (for good or ill).

Some governments and parts of governments "get it." One element that gets it is the U.S. Army, which in 2003 set up the Institute for Collaborative Biotechnologies. One area of focused research for the institute is "bio-inspired networks," studying "high-performance" biological networks for insights into how manmade networks can be made more scalable, robust, and energy efficient. In 2010, the institute oversaw 50 interdisciplinary research teams spanning 8 different academic departments at the Massachusetts Institute of Technology, University of California at Santa Barbara, and the California Institute of Technology. It is possible that the more scientists look to biological systems, the more applicable lessons they are finding for understanding computer systems and the activities on those systems, including social networking.

The potential of network science and its impact on social networks is too big an opportunity for free nations to ignore if they want to be respectable competitors in networked environments. All that said, while comparing cells and cellular phone networks sounds interesting, it is not easy science. A 2005 report by the U.S. National Academies laid out some daunting obstacles, including the difficulty in modeling and analyzing large, complex networks; developing better experiments and measurements of network structures; and establishing common concepts across the disparate disciplines that participate in network science.[13]

Seizing Cyber High Ground

Thinking about the future is a vital part of holding the cyber heights. Part of the answer is seizing and holding the initiative on knowledge creation. Concerning the competence of social networking, the foundation of knowledge discovery could well hinge on the capacity to conduct cutting-edge network science. Forecasting the future is equally important for serious cyber warriors. Social networking and other information technologies have greatly empowered the tools for understanding and appreciating how complex dynamic systems and competitions will unfold over time. Mastering these methods and combining them to form even richer insights will give competitors a unique edge in anticipating future challenges.

Finally, it is important to look over the horizon and begin to plan how to deal with future challenges. Knowing they are out there and doing nothing to either exploit them or prepare to counter them means a competitor will likely lose in the long run. The technology of social networking will remain as dynamic as the competition to harness it. If Washington does not develop the human capital to create first-class cyber leadership, it will wind up as an also-ran in the social networking war of warfare. **JFQ**

NOTES

[1] Josef Kolbitsch and Hermann Maurer, "The Transformation of the Web: How Emerging Communities Shape the Information We Consume," *Journal of Universal Computer Science* 2, no. 2 (2006), 187–207.

[2] John Palfrey, Bruce Etling, and Robert Faris, "Reading Twitter in Tehran?" *The Washington Post*, June 21, 2009, available at <www.washingtonpost.com/wp-dyn/content/article/2009/06/19/AR2009061901598.html>.

[3] Laura K. Donohue, "In the Name of National Security: U.S. Counterterrorist Measures, 1960–2000," BCIA Discussion Paper 20001–6, John F. Kennedy School of Government, Harvard University, August 2001.

[4] Jose Antonio Vargas, "Grading WhiteHouse.gov," *The Washington Post*, March 24, 2009.

[5] James Jay Carafano, *Social Networking and National Security: How to Harness Web 2.0 to Protect the Country*, Heritage Foundation Backgrounder No. 2273 (Washington, DC: The Heritage Foundation, May 18, 2009), available at <www.heritage.org/Research/NationalSecurity/bg2273.cfm#_ftn2>.

[6] Quotations from Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations* (New York: Penguin, 2008), 269, 271, 294.

[7] The spending estimate is based on National Communications System, Report 99–62, available at <www.ncs.gov/n5_hp/Customer_Service/XAffairs/NewService/NCS9962.htm>. For an overview of Y2K lessons learned, see David Mussington, *Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development* (Santa Monica, CA: RAND, 2002), 11–18.

[8] "Information Sharing Environment, Information Sharing Environment Implementation Plan," November 2006, available at <http://static/reportimages/AD829E9BA2DCE1A1A490FE89BF499CDD.pdf>.

[9] The Markle Foundation Task Force on National Security in the Information Age, "Nation at Risk: Policy Makers Need Better Information to Protect the Country," Washington, DC, March 2009, available at <www.markle.org/downloadable_assets/20090304_mtf_report.pdf>; Government Accountability Office (GAO), *Information Sharing Environment: Definition of the Results to Be Achieved in Improving Terrorism-Related Information Sharing Is Needed to Guide Implementation and Assess Progress*, GA0–05–492 (Washington, DC: GAO, June 2008), available at <www.gao.gov/new.items/d08492.pdf>.

[10] See Nicholas Evan Sarantakes, "Word Warriors: Information Operations during World War II," in *Mismanaging Mayhem: How Washington Responds to Crisis*, ed. James Jay Carafano and Richard Weitz (Westport, CT: Praeger, 2007), 27–45; Carnes Lord, "Marketing Freedom: Cold War, Public Diplomacy, and Psychological Warfare," in *Mismanaging Mayhem*, 46–66.

[11] Bryant Jordan, "Net Diplomacy," *Federal Computer Week*, October 29, 2000, available at <www.fcw.com/Articles/2000/10/29/Net-diplomacy.aspx>.

[12] See, for example, Committee on Network Science for Future Army Applications, *Network Science* (Washington, DC: The National Academies, 2005).

[13] Ibid., 48, 49.