War and the Media

Essays on News Reporting, Propaganda and Popular Culture

Edited by
PAUL M. HARIDAKIS,
BARBARA S. HUGENBERG *and*
STANLEY T. WEARDEN

McFarland & Company, Inc., Publishers
Jefferson, North Carolina, and London

ALSO OF INTEREST: *Sports Mania: Essays on Fandom and the Media in the 21st Century*. Edited by Lawrence W. Hugenberg, Paul M. Haridakis and Adam C. Earnheardt (McFarland, 2008)

LIBRARY OF CONGRESS ONLINE CATALOG DATA

War and the media : essays on news reporting, propaganda and popular culture / edited by Paul M. Haridakis, Barbara S. Hugenberg and Stanley T. Wearden.
p. cm.
Includes bibliographical references and index.

ISBN 978-0-7864-4607-0
softcover : 50# alkaline paper ∞

1. Mass media and war — United States. 2. War in mass media. 3. Popular culture — United States. 4. Mass media and public opinion — United States. 5. Mass media and propaganda — United States. I. Title. II. Haridakis, Paul M., 1957– III. Hugenberg, Barbara S., 1954– IV. Wearden, Stanley T.
P96.W352U5585 2009
070.4'4935502 — dc22 2009030616

British Library cataloguing data are available

Manufactured in the United States of America

McFarland & Company, Inc., Publishers
Box 611, Jefferson, North Carolina 28640
www.mcfarlandpub.com

TABLE OF CONTENTS

CYBERWAR: THE FUTURE OF WAR?

Brett Lunceford

When Estonian officials decided to remove Soviet war monuments from their capital in 2007, local Russians rioted and looted in protest. But the battle also took place online. An article in *The Economist* described the cyberattacks: "Some have involved defacing Estonian websites, replacing the pages with Russian propaganda or bogus apologies. Most have concentrated on shutting them down. The attacks are intensifying.... At least six sites were all but inaccessible, including those of the foreign and justice ministries" ("A Cyber-riot," 2007, p. 55).

Although these events seem relatively minor, such actions trouble the distinction between the physical world and the digital realm in the information age and raise questions concerning the potential for cyberspace to become an electronic battlefield.

> NATO has been paying special attention. "If a member state's communications centre is attacked with a missile, you call it an act of war. So what do you call it if the same installation is disabled with a cyber-attack?" asks a senior official in Brussels. Estonia's defense ministry goes further: a spokesman compares the attacks to those launched against America on September 11th 2001 ["A Cyber-riot," 2007, p. 55].

The full implications of information warfare are still being considered, but it seems that in an increasingly connected world such disruptions will become progressively more severe in impact.

The threat of hackers breaking into electronic systems has existed for quite some time, but the nature of the threat has evolved. In 1989, the Air Force Satellite Control Network System Program Office for Sustaining Engineering (1989) issued a pamphlet titled *The Hacker Threat* that portrays hack-

ers more as a nuisance than as a terrorist threat. Hackers are no longer seen as simply a nuisance. They are now potential terrorists or enemy combatants with the ability to destroy computerized systems from the relative anonymity of the ether. With the shift to an information economy comes the possibility that information can be used as a weapon, especially as the military becomes increasingly dependent on electronic communication systems and cryptography. McLuhan, Fiore, and Agel (1967/1996) prophetically declared that "real total war has become information war" (p. 138).

In this essay, I consider the potential for digital warfare to function as an appendage to traditional warfare. Cyberwar encompasses not only warfare against communication systems, but also warfare mediated through communication systems. Communication systems have always been a primary target in warfare, but now the attacks come not only from missiles but also from within the system. Moreover, the lines between citizen and enemy are no longer clearly demarcated. Individuals can do the work of armies in the digital realm through the use of programs and automation. Taking the battle into cyberspace allows an attacker to evade physical surveillance and disconnect from the body — possibilities inconceivable in industrial-age warfare. Communication systems are no longer simply the means by which one organizes forces in battle or wins the hearts and minds of the people — these systems are now part of the battlefield itself.

Defining Cyberwar

The practice of warfare is ever-evolving, often spurred on by combatants who attempt to use technological advances to achieve military superiority over those who lack that technology. For example, White (1962) suggested that the invention of the stirrup forever altered the nature of warfare, allowing for the possibility of mounted shock combat (pp. 1–38). Rothstein (2007) traced an evolution in American warfare strategies from massive land forces that were then coupled with naval forces and air power, through the advent of network-centric warfare (NCW) (pp. 277–278).

Modern military forces have evolved considerably from horse-mounted warriors. However, technologies tend to build on the past, augmenting previous practices rather than replacing them altogether. For example, despite its primitive origins, the infantry is still an important component of modern warfare, especially in the case of irregular warfare and guerrilla warfare where NCW may not be as effective (see Betz, 2006). Artillery and machinery, cast in the forge of the industrial age, continue to play an essential role in warfare. However, it is clear that the dawning of the information age will significantly influence the future of warfare (for theories concerning the information

society, see Bell, 1999; Castells, 2000; Schement, 1989; Schement & Curtis, 1997; Toffler, 1980, Webster, 1995). Communication systems are already an essential component of increasingly technologized warfare (see Schleher, 1999; Vakin, Shustov, & Dunwell, 2001).

Cyberwar is difficult to define, as it is sometimes used interchangeably with the terms netwar, information warfare, electronic warfare, cyberterrorism, hacking and net-centric warfare. Yan and Wang (2006) explained that "NCW is not only a campaign idea but also a campaign system ... centralizing command, control, communication, computer, intelligence, surveillance, and reconnaissance (C^4ISR), electronic warfare, information warfare, campaign support, and firepower system altogether, making [up] an information network system" (p. 121). Alexander (2008) provided this definition of cyberwar: "Cyberwar (CW) can be defined as a subset of the electronic order of battle (EOB) encompassing all operations that either attack computer systems and networks or defend against attacks, by aggressors, on friendly systems and networks" (p. 78). Arquilla and Ronfeldt (2001) defined netwar as "an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age" (p. 6). This is one of the more tailored definitions in that it accounts for the shifting ideologies that underlie modern warfare and recognize that the protagonists are no longer mainly agents of the state. It suggests that "these protagonists are likely to consist of dispersed organizations, small groups, individuals who communicate, coordinate, and conduct their campaigns in an internetted manner, often without a precise central command" (p. 6).

Cyberwar may be only one tactic among many in the practice of modern warfare, but it marks an important shift. The ideas of NCW, information war, electronic warfare, netwar, and cyberwar all point to a changing, increasingly digitized battlefield—a battlefield that is much more difficult to define in terms of civilian and military space. Brenner (2008) explained how the advent of cyberspace has brought about a significant shift in the ability to wage war, observing that "giving non-state actors access to a new, diffuse kind of power, cyberspace ends nation-states' monopolization of the ability to wage war and effectively levels the playing field between all actors" (p. 404). Arquilla and Ronfeldt (2001) also observed that "many—if not most—netwar actors will be nonstate, even stateless" (p. 7).

Although warfare is no longer the sole prerogative of the nation state, the kinds of warfare that can be waged by non–nation-state actors remain limited. In addition to isolated, but significant acts of terrorism, such as those performed on September 11, 2001, the potential exists for widespread disruption through infiltration of electronic networks. The cost of attacking another individual, group, or even nation-state in cyberspace is significantly lower than the cost of waging a similar attack in physical space. But the virtual and the physical have become intertwined, and attacks on the digital realm can ripple out into physical space. Nations and organizations that rely heavily on information technology systems are most vulnerable to cyberattacks (Gompert, Lachow, & Perkins, 2006, pp. 54–55).

It is now possible to distill some principles of cyberwar. First, *cyberwar is decentralized.* Cyberwar can be waged by small networks of individuals using sophisticated technology. Attacks can come from anywhere in the world with little warning. Second, *cyberwar mainly takes place in and through cyberspace.* As networks become increasingly important, they also become a more prominent target. During a hearing before the House Committee on Science, U.S. Congressman Bart Gordon stated,

> Networked information systems are key components of many of the Nation's critical infrastructures, including electrical power distribution, banking, finance, water supply, and telecommunications.... But we know that many international terrorist groups now actively use computers and the Internet to communicate, and they are clearly capable of developing or acquiring the technical skills to direct a coordinated attack against networked computers in the United States [*Cyber security: U.S. vulnerability*, 2005, p. 14].

Gordon underscored the potential for non-state actors to engage in attacks through digital space rather than physical space and the vulnerability of networked systems.

Third, *cyberwar exploits the interconnection between physical space and cyberspace.* Cyberwar is a product of the information age. Alexander (2008) noted that "with the increasing use of semi- and fully autonomous robotic surrogates for the soldier-in-the-loop in the battlespace, the cyberdomain is being exploited as a command and control interface with unmanned aerial vehicles (UAVs), unmanned underwater vehicles (UUVs) and battlefield robots" (p. 82). The interconnection between physical space and digital space makes it possible to engage in warfare remotely, thereby reducing risk to personnel. But anything that can be controlled remotely is vulnerable to intrusion or interference.

Considering the Future of Cyberwar Through Current Practice

In considering the future of cyberwar, it is illustrative to consider where we are presently. For the moment, I will propose an alternate definition of cyberwar: *cyberwar is the use of information technology to further the ends of*

warfare. I recognize that this is a broad definition, but broadening the scope of cyberwar allows for an exploration of some of the more mundane elements of cyberwar. With this definition, cyberwar encompasses the areas of communications, propaganda and psychological operations, funding operations, and intelligence. We will consider each, in turn.

Communications

Information technologies allow for an unprecedented ability to communicate in battle. One can communicate with friendly forces or intercept enemy communications to gather intelligence. Because of the importance of secrecy in tactical communications, cryptography has long been an important element of wartime communications, and information technologies provide new ways of encrypting messages (Gordon, 1981, pp. 14–25). Although early uses of cryptography were mainly in the hands of the government, it is increasingly used by the general public as well. This has altered the balance of power between the state and non-state actors. For example, cryptography has been used by those who fight against oppressive regimes (Jones, Kovacich, & Luzwick, 2002, p. 394). Cryptography also has been used by terrorist organizations to keep their transmissions secret, but the use of code can be decidedly lo-tech. Fielding (2004) reported that

> Al-Qaeda members have relied on simple encryption in ordinary e-mail exchanges. The September 11 hijackers, for example, while communicating between Europe and America, renamed the World Trade Center as the "faculty of town planning." Capitol Hill was the "faculty of law" and the Pentagon was the "faculty of fine arts." The date for the attack was also referred to openly in a simple code [p. 14].

Steganography is another way that information technologies allow for encryption. Steganography hides confidential information within another file. For example, a map can be embedded within another image or a document may be embedded within an mp3 music file. Most any digital file can be used to hide another digital file. For example, Polish researchers "were able to transmit 1.3Mbits of data in one direction during a 9-minute telephone call using the method, which relies on dropping bits into audio streams while retaining enough quality to make the call session useful to participants" ("Researchers Encode Secret Messages," 2008, p. 2). Thus, even wiretapping is no longer enough — one must consider the possibility that the message is embedded within the medium itself, rather than the spoken word that travels through the medium.

Steganography has clear benefits for terrorism and non-state sponsored attacks. Kolata (2001) reported that steganography "was used by recently apprehended terrorists who were planning to blow up the United States embassy in Paris. The terrorists were instructed that all their communications were to be made through pictures posted on the Internet" (p. F1). Other reports have suggested that Osama bin Laden has used cryptography and steganography in communications to operatives (Cha & Krim, 2001; Murphy, 2001). With steganography the casual observer sees only an image or hears a sound file. Only the intended recipient understands that there is a message within the file. Gary Gordon, vice president of digital forensics technology for WetStone Technologies, stated, "It's so insidious, you don't even know there is any communication going on" (quoted in Murphy, 2001, p. 5C).

As with most encryption schemes, the technology for resisting steganalysis is becoming more sophisticated. Liu and Liao (2008) proposed a method of embedding information within a JPEG image that resists several of the major attacks on steganography. This, coupled with the fact that steganography will easily hide an encrypted file, allows for a secure file to be hidden in plain sight. Thus, even if one can recognize that the file employs steganography, which may become more difficult as methods become increasingly sophisticated, the interceptor must then also break the encryption of the hidden file.

Impeding Enemy Communications

Information technologies can be used to impede an opponent's ability to disseminate their message. One example of silencing others can be found in the use of denial of service (DOS) attacks. At its most basic, a denial of service attack is overloading a server through the use of a zombie network or a script. Some hacktivists refer to this as a "virtual sit-in," because the effect is similar (Lane, 2003; Wray, 1999). Those who wish to enter cannot because the server is essentially full.

Denial of service attacks can also be used as a means of hackstortion, holding the server hostage unless demands are met (Conley, 2000). In 1999, a hacker collective called the electrohippies launched a denial of service attack against the World Trade Organization (WTO) during the WTO conference in Seattle. This provided an opportunity to raise consciousness concerning the actions of the WTO and allowed those who opposed the WTO to voice their arguments (DJNZ & Action Tool Development Group, 2000, pp. 7–8). Electronic Disturbance Theater also used this tactic to engage in politically motivated denial of service attacks on behalf of the Zapatista movement in Mexico (Lane, 2003; Wray, 1999).

The defacement of websites is another way that cyberwarriors can silence another's message while simultaneously disseminating their own.[1] A striking example of this took place on Sunday, September 13, 1998, when the *New York Times* website was hacked by a group of hackers called HFG, or H4cklng for Girl13s (Hacking for Girlies). The hack was a belated response to a 1994

New York Times article by John Markoff (1994) that portrayed Kevin Mitnick, a hacker, as a danger to society. However, Markoff was no mere beat reporter. Three years before writing the article for the *Times*, he had published a book that discussed Mitnick in great detail (Hafner & Markoff, 1991). By the time the hack occurred, Markoff had written another book and a screenplay describing Mitnick's capture and arrest (see Chappelle, 2000; Shimomura & Markoff, 1996). Thus, many hackers blamed Markoff for the demonization of Mitnick. The timing for the hack was well thought out. Kenneth Starr had just published his report to Congress concerning President Bill Clinton and Monica Lewinski. To regain control of the site, the *New York Times* had to take the site offline for most of the day. Bernard Gwertzman, editor of the *New York Times* on the Web, called it "the equivalent of somebody blowing up a press" (quoted in Noack, 1998, p. 55).

Propaganda and Psychological Operations

Information technologies also are used to disseminate propaganda. Ellul (1965) defined propaganda as "a set of methods employed by an organized group that wants to bring about the active or passive participation in its actions of a mass of individuals, psychologically unified through psychological manipulations and incorporated in an organization" (p. 61). According to Ellul, propaganda is too large an undertaking to be performed by one person. But, as information technologies have become more widespread it is now possible for individuals and small groups to disseminate messages and silence others.

According to Bernays (1928/2005), propaganda is about the management of an image, or "interpreting enterprises and ideas to the public, and ... interpreting the public to promulgators of new enterprises and ideas" (p. 63). One way this is done is through the use of websites. Dallal (2001) described how Hizballah has adapted their messages specifically for the Internet and how they have managed their image both through linking and as participants in a digital war against Israeli hackers. Even anarchists are organizing and using the Internet for damage control when they receive unfavorable news coverage related to anti-globalization protest actions (Owens & Palmer, 2003).

Terrorists, in particular, seem adept at using Internet communications as a way to gain attention from traditional mass media. For example, a communication from Osama bin Laden may be released on the Internet, then picked up by Al-Jazeera, and subsequently broadcast by CNN and other major U.S. news outlets. Of course, this requires some kind of interest in the message whether because of interest in the individual speaking — bin Laden, for example — or from a shocking display, such as the videotaped beheadings of Westerners (Colarik, 2006, pp. 50–51). Wagner (2005) wrote, "Along with satellite television, the web has turned out to be the preferred medium for

dissemination of terrorist 'information,' including news, propaganda, and other data that the terrorists would like to make available" (p. 21).

Terrorist organizations also have used websites as a tool to recruit potential members. Coll and Glasser (2005) reported,

> The Saudi Arabian branch of al-Qaida launched an online magazine in 2004 that exhorted potential recruits to use the Internet: "Oh Mujahid brother, in order to join the great training camps you don't have to travel to other lands," declared the inaugural issue of Muaskar al-Battar, or Camp of the Sword. "Alone, in your home or with a group of your brothers, you too can begin to execute the training program" [p. 10A].

Such an approach disseminates information much more efficiently than meeting in physical space while making it more difficult to identify who has taken part in such trainings. Sympathizers who may have been unable to participate due to lack of financial means or inability to travel can learn how to function as al-Qaida operatives where they already live. This allows for a wider, more diffuse network of potential operatives.

Funding Operations

In addition to disseminating information and recruiting potential operatives and sympathizers, information technologies also provide new ways to fund a group's or individual's actions, such as money laundering, especially through wire transfers (Shaffer, 2005; Wagner, 2005, pp. 22–23). The advantages of such a use of wire transfers are readily apparent, especially when conducted through non-mainstream bank entities. Transactions can be done anywhere in the world without being physically present.

Like other uses of information technology, money laundering can also be used in the service of mundane crime. A group of eleven hackers was indicted in 2008 for stealing over 40 million credit card numbers from various locations by breaking into computer systems and installing "sniffer" programs that gathered the data. They then encoded these onto blank cards and withdrew cash from ATM machines. CNN reported that the hackers "used anonymous Internet-based currencies to conceal and launder their proceeds, as well as channeling funds through bank accounts in Eastern Europe" ("Justice," 2008, paragraph 12). It is not difficult to see how terrorist organizations or other non-state opponents could employ similar methods to bankroll their activities.

Intelligence Gathering and Data Use

One area of cyberwar in which the government has a distinct advantage is intelligence gathering, especially in the use of data mining (Last, 2005). Seifert (2004) describes the core components of data mining as "the ability

to collect and combine, virtually if not physically, multiple data sources for the purposes of analyzing the actions of individuals" (p. 463). According to Seifert, "Data mining consists of more than collecting and managing data, it also includes analysis and prediction" (p. 464). But, as Seifert and Relyea (2004) observed, centralized databases provide "a rich target for hackers" (p. 403). When hackers gain access to these databases, they can gather considerable information, whether that information is intelligence concerning the plans of their enemies or simply the ability to engage in identity theft. Identity theft is the collateral damage of cyberwar. It is relatively unlikely that an individual will be targeted for identity theft. Rather, hackers tend to work in aggregates. Such information can be gathered in many ways. For example, at the University of California, Berkeley someone simply walked into an unlocked office and left with a laptop containing Social Security Numbers and information on over 98,000 former graduate students and applicants (Burress, 2005). On a more financial note, CardSystems, a credit card processing company, improperly kept data which resulted in 40 million credit card numbers being compromised, including the security check code that is supposed to deter fraudulent use (Dash, 2005). Savvy criminals can even buy information. ChoicePoint sold access to 145,000 consumer records to thieves who presented themselves as small business owners (Zeller, 2005).

All of these examples demonstrate the potential for groups and individuals to use financial and personal information that the affected individuals may not have even known existed. These digital activities may also spill over into physical space. In her discussion of identity theft, McCue (2005) stated, "After 9/11, it became painfully obvious that the highjackers had easily obtained the false credentials necessary to move throughout the many systems that require identification" (pp. 53–54).

Viruses as Weapons

There are ways that cyberwar could theoretically be waged by exploiting code flaws in software. One such way is through the use of a computer virus. Computer viruses have been around since at least 1983, when Fred Cohen invented what is generally considered to be the first computer virus (Jones, et al., 2002, p. 498). Viruses, worms, and other malware are a concern to many because of our reliance on information technology. Hughes and DeLone (2007) argued that discourse concerning viruses range from dangers that are "widely touted, by the media, the government, and others" to a "growing chorus of voices criticizes this position for being based on an irrational fear of what often turns out to pose little to no real threat" (p. 92). Hughes and DeLone's study suggests that both sides have an element of truth to them (p. 93).

Although the impact of computer viruses can be significant, assessment of actual cost of damages varies widely. For example, Colarik (2006) stated that the Love Bug virus reportedly caused $3–15 billion in damages worldwide (pp. 86–87). Hinde (2000) reported the estimate at $100 million to $10 billion in worldwide damages, but observed, "Now that looks a pretty accurate estimate! This compares to Computer Economics' estimate that $12.1 billion in damages were incurred worldwide due to viruses in all of 1999" (p. 408).

Although viruses could be used for warfare, perhaps the threat is overstated. Most security breaches come not from external hackers, using viruses and other tools, but from employees or former employees. Perry (2006) reported that the "DTI Information Security Breaches Survey found that the average cost to large businesses of a major security incident was more than $170,000—and 87 percent of them had experienced a breach," but that the threat from the inside of an organization is considerably higher than threats from the outside (p. 11). Perry concluded, "Whatever the true cost, internal threats certainly cost millions more every year than losses from viruses or spyware" (p. 11; see also, "IP Theft Costs," 2003, p. 3).

Although viruses receive a lot of press and are highly visible when they occur, combatants are more likely to exploit existing flaws in the software or use other programs to gain access to the network. Viruses work mainly as a way to temporarily disable a network and would therefore remain useful from the perspective of cyberwar, but in a more limited capacity than the fear surrounding them would indicate. Combatants may be more interested in keeping the network open, especially if they wish to intercept enemy communications. Moreover, viruses are difficult to control once they are released and may hinder friendly systems as well as those of the enemy.

Cyberwar as an Appendage to Conventional Warfare

Where cyberwar has the greatest chance of impact is as an appendage to conventional warfare. Arquilla and Ronfeldt (2001) explained that

> netwar is not simply a function of 'the Net' (i.e., the Internet); it does not take place only in "cyberspace" or in the "infosphere." Some *battles* may occur there, but a *war's* overall conduct and outcome will normally depend mostly on what happens in the "real world"—it will continue to be, even in information age conflicts, generally more important than what happens in cyberspace or the infosphere [p. 11].

Cyberwar's power, in part, comes from the ability of non-state actors to take the battle to a more level playing field in cyberspace. Oxblood Ruffin (2000), a member of the hacker collective Cult of the Dead Cow, argued,

"Where a large physical mass is the currency of protest on the street, or at the ballot box, it is an irrelevancy on the Internet.... Programs make a difference, not people" (paragraph 18). Separating the programs from the people implies a significant shift in warfare and protest.

The possibilities of electronic systems to alter the balance of power between the nation state and groups of citizens can be found in the study of social movement protest actions in which protesters use technology to integrate digital strategies with physical action. Kahn and Kellner (2004) explained that social movements are becoming increasingly technologically savvy, with members using cell phones, personal digital assistants (PDAs), global positioning systems (GPS), laptops, wireless internet access, and engaging in actions such as wardriving and blogging to disseminate their message. The anti-globalization movement in particular has made significant use of new media as a way to forward its goals and enhance its protest actions (e.g., DeLuca & Peeples, 2002; Juris, 2005; Kahn & Kellner, 2004; Van Aelst & Walgrave, 2002).

Rheingold (2002) suggested that individuals can be brought together as "smart mobs" through a mixture of technologies such as mobile phones, wireless Internet, text messaging systems, and blogging. According to Rheingold, smart mobs "cooperate in ways never before possible because they carry devices that possess both communication and computing capabilities" (p. xii). In one striking example, Rheingold called President Joseph Estrada of the Philippines, who had just had his impeachment proceedings stopped by supporters, "the first head of state in history to lose power to a smart mob" (p. 157). According to Rheingold,

> Tens of thousands of Filipinos converged on Epifanio de los Santas Avenue, known as "Edsa," within an hour of the first text message volleys: "Go 2EDSA, Wear blck." Over four days, more than a million citizens showed up, mostly dressed in black. Estrada fell. The legend of "Generation Txt" was born [Rheingold, 2002, pp. 157–158].

The diffusion of mobile technologies such as cellular phones, wireless internet, text message systems (SMS) and interconnected devices such as personal digital assistants (PDA) and global positioning system (GPS) units allow groups to function as united bodies, especially when combined with websites generating RSS (Really Simple Syndication) feeds which provide constantly updated information from a centralized location. Such technologies are important when opposing a militarized police force equipped with tactical communication systems and help to shift the balance of power. Although the end result in Rheingold's example — physical protest — is similar to previous social movement actions, the means by which it is conducted and organized have become more efficient, more tactical.

Concluding Postscript

As I wrote this conclusion, Russia and Georgia were locked in a conflict that included both physical attacks and cyber attacks. Don Jackson, director of threat intelligence for SecureWorks, explained that "in the run-up to the start of the war over the weekend, computer researchers had watched as botnets were 'staged' in preparation for the attack, and then activated shortly before Russian air strikes began on Saturday" (quoted in Markoff, 2008, paragraph 15). In an illustration of how difficult it is to trace the protagonists in cyberwar, Markoff (2008) reported, "Exactly who was behind the cyberattack is not known" (Paragraph 8). It seems that cyberwar is not the future of war; cyberwar is now just another component of modern warfare. Thus, the future of war is likely to be an age old story — the violent deaths of men, women, and children as people continue to march to the battlefield. Cyberwar only expands the battlefield and allows more people to enter.

Note

1. Website defacement is quite common. For example, in the week ending August 2, 2008, Zone-h, a cyber security site, reported 9,717 website defacements. This is only a representation of defacements that were reported. For up to date information on website defacements, view the attack archive at www.zone-h.org.

References

A cyber-riot. (2007, May 12). *The Economist*, p. 55.

Air Force Satellite Control Network System Program Office for Sustaining Engineering (1989). *The Hacker Threat*. Washington, DC: Air Force Satellite Control Network System Program Office for Sustaining Engineering.

Alexander, D. (2008). Cyberwar comes of age. *Military Technology, 32*(3), 78–85.

Arquilla, J., and D. F. Ronfeldt (2001). The advent of netwar (revisited). In J. Arquilla & D. F. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp. 1–25). Santa Monica, CA: Rand.

Bell, D. (1999). *The Coming of Post-Industrial Society: A Venture in Social Forecasting* (Special anniversary ed.). New York: Basic.

Bernays, E. L. (2005). *Propaganda*. Brooklyn, NY: Ig. (Original work published 1928.)

Betz, D. (2006). The more you know, the less you understand: The problem with information warfare. *Journal of Strategic Studies, 29*, 505–533.

Brenner, S. W. (2007). "At light speed": Attribution and response to cybercrime/terrorism/warfare. *Journal of Criminal Law & Criminology, 97*, 379–475.

Burress, C. (2005, March 29). Berkeley / Cal issues alert about stolen laptop computer / It contains 98,000 Social Security numbers — notifications to warn of identity-theft risk. *San Francisco Chronicle*, p. B1.

Castells, M. (2000). *The Rise of the Network Society* (2nd ed.). Oxford: Blackwell.

Cha, A. E., and J. Krim (2001, September 19). Terrorists' online methods elusive; U.S. agencies seek experts' help in tracing encrypted messages. *The Washington Post*, p. A14.

Chappelle, J. (Director). (2000). *Track Down* [Motion picture]. United States: Dimension Home Video.

Colarik, A. M. (2006). *Cyber Terrorism: Political and Economic Implications*. Hershey, PA: Idea Group.
Coll, S., and S. B. Glasser (2005, August 7). Jihadists make Web base for recruiting, training. Ease, portability boost movement. *Journal-Gazette*, p. 10A.
Conley, J. (2000). Outwitting cybercriminals. *Risk Management, 47*(7), 18–26.
Cyber Security: U.S. Vulnerability and Preparedness: Hearing Before the Committee on Science, House of Representatives, 109th Cong., 1 (2005).
Dallal, J. A. (2001). Hizballah's virtual civil society. *Television & New Media, 2*, 367–372.
Dash, E. (2005, June 20). Lost credit data improperly kept, company admits. *New York Times*, p. A1.
DeLuca, K. M., and J. Peeples (2002). From public sphere to public screen: Democracy, activism, and the "violence" of Seattle. *Critical Studies in Media Communication, 19*, 125–151.
DJNZ, & Action Tool Development Group of the electrohippies collective (2000, February). *Occasional Paper No. 1: Client-Side Distributed Denial-of-Service: Valid Campaign Tactic or Terrorist Act?* Retrieved January 30, 2006, from http://www.fraw.org.uk/ehippies/papers/op1.pdf.
Ellul, J. (1965). *Propaganda: The Formation of Men's Attitudes* (K. Kellen & J. Lerner, Trans. 1st American ed.). New York: Knopf.
Fielding, N. (2004, August 8). Al-Qaeda betrayed by its simple faith in high-tech. *Sunday Times*, p. 14.
Gompert, D. C., I. Lachow, and J. Perkins (2006). *Battle-wise: Seeking Time-Information Superiority in Networked Warfare*. Washington, DC: Center for Technology and National Security Policy, National Defense University Press.
Gordon, D. E. (1981). *Electronic Warfare: Element of Strategy and Multiplier of Combat Power*. New York: Pergamon.
Hafner, K., and J. Markoff (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster.
Hinde, S. (2000). Love conquers all? *Computers & Security, 19*, 408–420.
Hughes, L. A., and G. J. DeLone (2007). Viruses, worms, and Trojan horses: Serious crimes, nuisance, or both? *Social Science Computer Review, 25*, 78–98.
IP theft costs overtake virus losses. (2003). *Computer Fraud & Security, 2003*(6), 3.
Jones, A., G. L. Kovacich, and P. G. Luzwick (2002). *Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages*. Boca Raton, FL: Auerbach.
Juris, J. S. (2005). The new digital media and activist networking within anti-corporate globalization movements. *The Annals of the American Academy of Political and Social Science, 597*, 189–208.
Justice: Hackers steal 40 million credit card numbers. (2008, August 5). *CNN.com*. Retrieved August 6, 2008, from http://www.cnn.com/2008/CRIME/08/05/card.fraud.charges/.
Kahn, R., and D. Kellner (2004). New media and internet activism: From the "battle of Seattle" to blogging. *New Media & Society, 6*, 87–95.
Kolata, G. (2001, October 30). Veiled messages of terror may lurk in cyberspace. *New York Times*, p. F1.
Lane, J. (2003). Digital Zapatistas. *TDR: The Drama Review, 47*, 129–144.
Last, M. (2005). Using data mining technology for terrorist detection on the web. In M. Last & A. Kandel (Eds.), *Fighting Terror in Cyberspace* (pp. 41–62). Hackensack, NJ: World Scientific.
Liu, C.-L., and S.-R. Liao (2008). High-performance JPEG steganography using complementary embedding strategy. *Pattern Recognition, 41*, 2945–2955.
Markoff, J. (1994, July 4). Cyberspace's most wanted: Hacker eludes F.B.I. pursuit. *New York Times*, pp. A1, A36.

Markoff, J. (2008, August 12). Before the gunfire, cyberattacks. *New York Times*. Retrieved August 14, 2008, from http://www.nytimes.com/2008/08/13/technology/13cyber.html.
McCue, C. (2005). Data mining and predictive analytics: Battlespace awareness for the war on terrorism. *Defense Intelligence Journal, 13*(1&2), 47–63.
McLuhan, M., Q. Fiore, and J. Agel (1996). *The Medium Is the Massage: An Inventory of Effects*. San Francisco, CA: HardWired. (Original work published 1967.)
Murphy, K. (2001, October 11). Hidden messages used to plan attacks? *The Charleston Gazette*, p. 5C.
Noack, D. (1998, September 19). Hack attack sends chill through news Web sites. *Editor & Publisher, 131*, 14, 55.
Owens, L., and L. K. Palmer (2003). Making the news: Anarchist counter-public relations on the world wide web. *Critical Studies in Media Communication, 20*, 335–361.
Oxblood Ruffin. (2000, July 17). *Hacktivismo*. Retrieved November 17, 2008, from http://w3.cultdeadcow.com/cms/2000/07/hacktivismo.html.
Perry, S. (2006). Network forensics and the inside job. *Network Security, 2006*(12), 11–13.
Researchers encode secret messages in VoIP calls. (2008). *Network Security, 2008*(7), 2.
Rheingold, H. (2002). *Smart Mobs: The Next Social Revolution*. Cambridge, MA: Perseus.
Rothstein, H. S. (2007). Less is more: The problematic future of irregular warfare in an era of collapsing states. *Third World Quarterly, 28*, 275–294.
Schement, J. R. (1989). The origins of the information society in the United States: Competing visions. In J. L. Salvaggio (Ed.), *The Information Society: Economic, Social, and Structural Issues* (pp. 29–50). Hillsdale, NJ: Lawrence Erlbaum.
Schement, J. R., and T. Curtis (1997). *Tendencies and Tensions of the Information Age: The Production and Distribution of Information in the United States*. New Brunswick, NJ: Transaction.
Schleher, D. C. (1999). *Electronic Warfare in the Information Age*. Boston: Artech House.
Seifert, J. W. (2004). Data mining and the search for security: Challenges for connecting the dots and databases. *Government Information Quarterly, 21*, 461–480.
Seifert, J. W., and H. C. Relyea (2004). Do you know where your information is in the homeland security era? *Government Information Quarterly, 21*, 399–405.
Shaffer, Y. (2005). Analysis of financial intelligence and the detection of terror financing. In M. Last & A. Kandel (Eds.), *Fighting Terror in Cyberspace* (pp. 105–116). Hackensack, NJ: World Scientific.
Shimomura, T., and J. Markoff (1996). *Take-down: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw — by the Man Who Did It*. New York: Hyperion.
Toffler, A. (1980). *The Third Wave*. New York: William Morrow.
Vakin, S. A., L. N. Shustov, and R. H. Dunwell (2001). *Fundamentals of Electronic Warfare*. Boston, MA: Artech House.
Van Aelst, P., and S. Walgrave (2002). New media, new movements? The role of the internet in shaping the anti-globalization movement. *Information Communication & Society, 5*, 465–493.
Wagner, A. R. (2005). Terrorism and the internet: Use and abuse. In M. Last & A. Kandel (Eds.), *Fighting Terror in Cyberspace* (pp. 1–28). Hackensack, NJ: World Scientific.
Webster, F. (1995). *Theories of the Information Society*. London: Routledge.
White, L., Jr. (1962). *Medieval Technology and Social Change*. Oxford: Oxford University Press.
Wray, S. (1999). On electronic civil disobedience. *Peace Review, 11*, 107–111.
Yan, T., and B. Wang (2006). Grid architecture model of network centric warfare. *Journal of Systems Engineering and Electronics, 17*, 121–125.
Zeller Jr., T. (2005, March 5). Release of consumers' data spurs ChoicePoint inquiries. *New York Times*, p. C2.