Information Warfare: Its Application in Military and Civilian Contexts

Blaise Cronin and Holly Crawford

School of Library and Information Science, Indiana University, Bloomington, Indiana, USA

BELTWAY BUZZWORDS

The lexicon of information warfare (IW), or cyberwar, to use a common variant, has been around for more than two decades (Adams, 1998), but for most of that time it has remained the preserve of the defense community. Within the cloistered world of the Pentagon and its satellite communities, a radically new concept of postindustrial warfare has crystallized, one that is designed to ensure continued U.S. military dominance in the post-Cold War era. There exists an extensive literature on information warfare theory and practice, much of which is in the public domain (De Landa, 1991; Libicki, 1995; Schwartau, 1996; Denning, 1999). Predictably, the prevailing language, images, and metaphors are classically militaristic in character, blurring the fact that many of the underpinning principles and assumptions have application well beyond conventional military contexts. This privileging of military thinking is myopic. Information warfare concepts deserve to be liberated from their military associations and introduced into other discourse communities concerned with understanding the social consequences of pervasive computing. Already, the principles and practices of information warfare are being exhibited, more or less wittingly, in a variety of civilian contexts (from computer-based fraud to cyberstalking), and there are good grounds for assuming that this trend will intensify, causing potentially serious social problems and creating novel challenges for the criminal justice system. To paraphrase a well-worn cliché, information warfare is too important to be left to the military.

INFORMATION WARFARE

The term “information warfare” is still popularly associated with high-technology weapons and broadcast images of Cruise missiles seeking out Iraqi or Serbian military targets with apparently unerring accuracy. Armchair viewing of arm’s-length battles has created a simplistic and sanitized vision of information warfare in which, to paraphrase Toffler (1990), the mindless fist is replaced by congealed mind. The media’s early focus on smart bombs and intelligent battle systems—the tangible paraphernalia of the digital battle space—masked the potentially deeper societal implications of virtual warfare strategies. That, however, is beginning to change, as journalists and pundits foreground computer hacking and data corruption as pivotal information warfare techniques. Simplifications and confusions notwithstanding, an axial assumption of information age warfare is that brains matter more than brawn. In tomorrow’s battlefield, be it military or civilian, information technology will act as a force multiplier. Traditional notions about the bases of superiority and power dynamics existing between attacker and target may thus require redefinition.

Pandemic access to digital networks creates a downward adjustment of established power differentials at all levels of society. Traditional notions of combat assume some parity in terms of payload and starting ratios: A platoon does not go head-to-head with a battalion, a small business does not take on a Fortune 500 company, and a bantamweight does not challenge a sumo wrestler. Of course, history is littered with exceptions to this rule of thumb—partisan groups, guerrilla movements, aggressive start-ups. In the electronic arena, however, axial assumptions about force parity do not necessarily hold. Military might is demassified, and a digital David can indeed challenge a seemingly PGP-protected Goliath, almost with impunity. This is what Cusumano and Yoffie (1998), in another context, call the judo strategy, that is to say, turning

Received 11 February 1999; accepted 15 February 1999.

We are grateful to Elisabeth Davenport, Rob Kling, and Debora Shaw for their comments.

Address correspondence to Blaise Cronin, School of Library and Information Science, Indiana University, Bloomington, IN 47405-1901, USA. E-mail: bcronin@indiana.edu

The Information Society, 15:257–263, 1999
Copyright © 1999 Taylor & Francis
0197-2243/99 $12.00 + .00

TABLE 1
Information warfare

Target	Actions
Physical assets	Damage or destroy target's information and communication systems using conventional warfare techniques
Soft assets	Infiltrate, degrade, subvert information systems; use external actors and corrupted insiders to crack firewalls and degrade target's information systems capability, using malicious software
Psychic assets	Silent penetration of target's information and communications systems to manage perceptions, shape opinions, foster deception, and engage in epistemological warfare

the enemy's size—in this instance computing muscle—to the attacker's advantage.

The principles and practice of information warfare (Table 1), though eagerly embraced by various branches of the armed services (e.g., Molander et al., 1996) have potentially much wider implications for society at large in a networked age, a point made in the fall 1995 issue of the *Rand Research Review*, which was devoted to information war and cyberspace security (http://www.rand.org/publications/RRR/RRR.fall95.cyber/). Here we consider four spheres of activity in which information warfare may very soon become relatively commonplace: military, corporate/economic, community/social, and personal. Certain IW concepts, strategies, and applications are common to all four settings, though there may be interpretative differences, as well as differences in the perceived legality, ethicality, and social desirability of the outcomes pursued by different actors under different conditions. Our intention is to provide an analytic framework for understanding key dimensions of information warfare and some of the myriad social ramifications arising from the co-option of internetworking technologies for the conduct of IW campaigns, be they military or civil, collective or individualistic, systematic or aleatory in character.

THE MILITARY CONTEXT

The term "information warfare" is widely, though inconsistently, used within the U.S. defense community, where rhetorical gamesmanship and interservice rivalries are never far from the surface, as the various stakeholders contest ownership and control of the IW agenda. The Pentagon is making significant investments in the development of IW strategies (both offensive and defensive) and the associated digital technologies in an effort to augment the nation's comparative military advantage. However, there are still informed skeptics within the military ranks, who dismiss IW theory as "a wonkish vision of war . . . more convincing to defense contractors than to America's enemies" (Peters, 1998, p. 39).

Simply put, information warfare implies a range of measures or "actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary" (Alger, 1996, p. 12). A typical goal of conventional warfare is to destroy or degrade the enemy's physical resources, whereas the aim of IW is to target information assets and infrastructure, such that the resultant damage may not be immediately visible or detectable to the untrained eye: These strikes are called soft kills. In practical terms, cyberwarfare means infiltrating, degrading, or subverting the target's information systems using logic bombs or computer viruses. But it also extends traditional notions of psychological warfare: An IW goal may be silent penetration of the target's information and communications system in order to shape community perceptions, foster deception, or seed uncertainty—what is known as epistemological, or neocortical, warfare (Szafranski, 1994).

Propaganda and disinformation campaigns have long been staples of conventional warfare. In the battle for hearts and minds, the control of broadcast technologies (television, radio) has been a prime objective. In one sense, nothing much has changed, but the picture has become more complicated with the emergence of the Internet and World Wide Web, which give voice to the most unlikely individuals and groups, their multidirectional communication properties affording access to audiences that, under monopolistic or oligopolistic broadcasting conditions, would have remained permanently out of reach. In the information age, the silent enemy can easily acquire a voice and quickly amplify its dissident message. Unidirectional channels are being displaced by rhizomic communication patterns, which render the urge to control and censor almost futile.

Apart from the low cost of entry, the would-be attacker's advantages (Table 2) include the ease, swiftness, and stealth with which a determined assault can be mounted, as well as the scope or reach afforded by global networks (Meinel, 1998). No longer need either distance or the "friction of the whole machine," to quote Carl von Clasusewitz (1967), impair the would-be attacker. Geography, terrain, and logistics drop out of the calculus; the combat zone is, theoretically, anywhere on the network. Perhaps the most important element of information warfare

TABLE 2
Aspects of information warfare

- Low-intensity operations
- Targeting of soft assets
- Asymmetrical payloads and starting ratios
- Zero warning/latency
- Use of logic bombs and computer viruses
- IT sophistication correlates with pregnability
- Offensive and defensive IW
- Critical infrastructure vulnerability
- Attacker dictates rules of engagement
- Ambiguous "weapons effects"
- Intelligence blind spots
- Premium on strategic intelligence

Note: IT, information technology.

is the near unknowability of the attacker coupled with nagging uncertainty as to his driving motivations. An information warrior, like the F16 fighter pilot who releases his laser-guided missiles out of sight and range of the target (stand-off, in military terminology), can enjoy a sense of impersonality and anonymity in his engagement with the enemy (Table 3).

Of course, IW constitutes a double-edged sword for information-intensive nations like the United States. The greater the military's reliance on complex networks and smart weaponry, the greater is its potential vulnerability to stealth attack by materially much weaker enemies blessed with networking savvy, be they foreign agents or corrupted insiders. And it is this aspect of IW—resource asymmetricality—that has attracted so much attention among both military planners and media analysts and shifted much of the discussion from offensive to defensive information warfare strategy. In addition, there is the absence of early warning and the difficulty of knowing whether, or to what extent, one's systems have been penetrated and compromised—in military parlance, confusion as to "weapons effect," the actual damage cause by a particular weapon or attack strategy. It can also be a challenge for the target to distinguish national-scale attacks from intrusions that are of essentially local import.

In theory, a small team of hackers (even a lone operator) can wreak havoc, whether the target is military or civilian, as Stoll (1984) has compellingly documented. Today, the U.S. Department of Defense computer systems are subjected to hundreds of thousands of attacks each year (Boulanger, 1998). Fear of an electronic Pearl Harbor has stimulated public debate on the vulnerability of the nation's econotechnical information infrastructure (Schwartau, 1996) to cyber-attacks and led to the establishment in 1996 of the Commission on Critical Infrastructure Protection (http://www.pccip.gov/). In information technology-based warfare, the attacker is much more likely to achieve strategic surprise than in conventional forms of military engagement (Handel, 1995).

TABLE 3
Attacker advantages

- Attacker typically invisible to target
- Swift strike advantage
- Fluidity of attack mode
- Ability to vary frequency and intensity of attack
- Multiple effects available to attacker
- Scalability easily achieved
- Ease with which allies can be mobilized
- Target placed in reactive mode
- Target has to contain collateral damage
- Target's behaviors forcibly changed
- Ethical and legal ambiguities

CORPORATE/ECONOMIC INFORMATION WARFARE

The language of business is no less revealing. Within the North American MBA (master's degree in business administration) culture, for instance, competition is the dominant metaphor, and management textbooks are replete with military terminology and warfare analogies—flanking strategies, guerrilla marketing, price wars, competitor intelligence, killer applications, first-strike advantage. And not without reason: "The similarities between the military and business world grow each day. Both involve competition between adversaries with various assets, motives, and goals. Enemy surveillance and competitive intelligence are *de rigueur* in both fields" (German et al., 1991, p. 78). With the progressive globalization of trade and internationalization of business, the parallels will intensify (Cronin & Crawford, 1999). Business would thus seem to be an obvious site to appropriate the discourse of information warfare, as McCrohan (1998) clearly suggests. Given the growing dependence of companies on sophisticated information systems, and, more particularly, the rapid growth of Web-based electronic commerce, it is reasonable to conclude that information warfare theory will soon establish a curricular foothold in leading business schools.

From the perspective of a foreign enemy, ethnoterrorist, or internal dissident, an attack on high-visibility corporate assets could generate as much symbolic resonance as a full-frontal assault on a conventional military or civil target. Consider the immediate consequences and ripple effects of a successful cyber-attack on MasterCard's main computer system, a Trojan Horse virus inserted into

American Airline's computerized customer reservation system, or systematic contamination of patient records held in the Mayo Clinic. If such can be achieved remotely by dedicated hackers without risk to life or limb, and without committing tangible military resources, it is not hard to see the attraction of offensive IW strategies in the context of global economic warfare.

A corollary of such presumed pregnability is heightened corporate awareness of the need for systems integrity in order to prevent sabotaging of mission-critical or proprietary information by competitor companies or foreign governments (Fialka, 1997). Corporations have little choice but to commit resources to defensive information warfare strategies in an effort to protect themselves against theft, disruption, distortion, denial of service, or destruction of sensitive information assets. This does not simply mean building stronger firewalls, enhancing existing encryption procedures, or installing software that launches counterattacks (Yasin, 1998), but investing resources in creating more effective intelligence and counterintelligence capability in an effort to anticipate likely attacks and their sources (Bar-Joseph & Sheaffer, 1998). To quote Toffler and Toffler (1993), "knowledge warfare involves shaping enemy action by manipulating the flow of intelligence and information." In an age of economic and corporate information warfare, proactive intelligence management systems become essential requirements for high-performing companies, as evidenced, for example, by the growing role played by the National Counterintelligence Center in providing U.S. private-sector firms with guidance and advice on how to cope with foreign intelligence threats to their business operations (http://www.nacic.gov/).

Sometimes the "enemy" will be bona fide consumers with legitimate grounds for complaint. The ease with which a disgruntled customer, or group of customers, can vent their spleen and mobilize support on the Web to challenge the reputation of a firm presents new problems for corporate public relations, marketing, and advertising departments. In electronic markets, shoddy goods, broken promises, falsity in advertising, or price gouging may be enough to trigger an orchestrated retaliation campaign, or class action suit, from disaffected customers versed in the art of Web-based information warfare. In Web wars, the vulnerability of reputations (personal, product, institutional) will be a critical variable. The Pentagon does not want to be embarrassed by high-profile hacking of its national security systems, the large tobacco companies do not want their internal memoranda and potentially incriminating research papers to be posted on public Web sites by antismoking campaigners, and university scholars do do want to be victims of smear campaigns that question the integrity of their research and publication record or the quality of their classroom instruction.

COMMUNITY/SOCIAL INFORMATION WARFARE

The rise of the networked society has resulted in an intensification of debate on a vast array of social issues. Nowhere is this online war of words more evident than in the United States (Cronin, 1998). Early studies show that highly active online users are strongly libertarian in character and passionately convinced of the ability of business and individuals— not government—to solve the problems of the day (Katz, 1997). It is easy to see how group identity can be swiftly engineered, empowered, and reinforced using distributed computing: Lone voices quickly find their echo, and a sense of incipient control can soon crystallize—the force multiplier effect. The step from benign lobbying and belligerently challenging the status quo to digital anarchy is a short one.

What makes distributed computing, or more specifically the Internet, so attractive to individuals or groups interested in having their opinions heard or waging word warfare with others is the lack of restraints. Gatekeeping, particularly in the public sphere, is not a new concept. The colonialists subsidized newspapers so that government information could reach a wider audience. Printers routinely printed what the government wanted for fear of libel and the negative economic consequences of losing their largest customer (Boorstein, 1958). The Federal Communications Commission (FCC) regulates the content of radio and television broadcasts to such a degree that some see little evidence of free speech, a constitutional guarantee and right. Government control of the Internet, however, has not followed that of newspapers, radio, and television. Although there have been (and continue to be) legislative attempts to control Internet content (e.g., Communications Decency Acts I and II), these have been thwarted by advocates of free speech and intellectual freedom, notably the American Civil Liberties Union (ACLU) and the American Library Association (ALA). Consequently, the Internet remains a communications arena where discourse, positive and negative, rational and irrational, flourishes freely.

The halcyon days of networked computing saw the proliferation of electronic bulletin boards like The Well. These digital granges (town meetings) allowed individuals and diverse or marginalized groups of people to exchange ideas on everything from gardening tips to AIDS-related health issues. Militant activist groups such as PETA (People for the Ethical Treatment of Animals) and Act Up, a gay and lesbian organization determined to attain equal rights for its constituents, used bulletin boards as one of their earliest assault weapons for inexpensive and widespread expression of their opinions. Strategy and tactics as such did not come into play; blanket dissemination was the goal. One could liken this to the Allies using B-29s to litter the German countryside with propaganda leaflets during World War II. In similar vein, Microsoft employees are, allegedly, encouraged to post to Z-Net articles using fictional names (while pretending to be students) in order to promote their company's actions and credibility—http://www.zdnet.com/talkback/22_26562_108781.html. Once upon a time this would have been labeled propaganda; today it is more likely to viewed as a defensive information warfare tactic by a seemingly beleaguered corporation.

While bulletin boards and their progeny, IRC, MUDs, and MOOs, have allowed for the free exchange of ideas, they have also opened up the digital environment to groups keen on waging their own brand of cyberwarfare. On traditional battlefields, soldiers use flamethrowers to repel attackers; in cyberspace, one "flames" enemies, real or imagined, with ASCII text. Many Russian military songs lament the raping of women and the pillaging of villages by warring Slavic tribes hundreds of years ago. Today one can read the story of the first cyber-rape, which took place in LambdaMOO, a virtual village built out of C code (Dibbell, 1993).

With the advent of the World Wide Web and graphical user interfaces or browsers such as Netscape, social and political activists have an even richer agora in which to debate, pontificate, or castigate (Brophy et al., 1998). Religiously or ideologically motivated groups now have at their disposal the means of waging electronic jihad. Recent use of the Web by pro-life groups in the United States can be analyzed in terms of First Amendment issues and ethics—or it can be viewed as a harbinger of the imminent militarization of social and ideological activism. But the phenomenon is by no means restricted to the United States. In January 1999, the Indonesian government was blamed for a systematic attack on computers in the Republic of Ireland that brought down the East Timor virtual country domain. According to the target, Connect-Ireland, there were 18 simultaneous attacks on the company's server by robots trying to breach the company's defenses (http://news.bbc.co.uk/hi/english/sci/tech/newsid_263000/263169.stm). In Indonesia, web sites have been attacked by campaigners protesting the treatment of that country's ethnic Chinese population (http://news.bbc.co.uk/hi/english/sci/tech/newsid_154000/154079.stm).

Of course, the use of the Web by political or social activists need not necessarily result in undesirable outcomes. There is evidence that digital communication technologies are accelerating the emergence of a third, or social, sector alongside the established public and private sectors (Arquila & Ronfeldt, 1996). In theory, cyberlobbying/activism is just as capable of producing beneficial results as it is of having a corrosive and dissipative effect on society. However, given that the Web allows for the promulgation of multiple viewpoints, there is a risk that the social glue that holds nation-states together may weaken, resulting in a plethora of competing microagendas and localized value systems. Ten years ago, researchers with the Office of Technology Assessment (OTA) predicted this possibility: "Not only will new groups be established outside of traditional political channels; within existing groups, there is likely to be a shift in the chain of command . . . to the extent that electronic bulletin boards are employed to target specific people, they could lead to the fragmentation of the body politic" (OTA, 1990, p. 169). For a pluralistic nation like the United States, loss of social cohesion and a common sense of identity could thus be the ironic price of digital democracy in extremis.

How has this situation arisen? It is clear that delayering and disintermediation—the loss of intervening controls, such as editors, fact checkers, reputable publishers, social filters, verifying agencies, peer reviewers, and quality controllers—have created a climate conducive to information warfare and cyber-terrorism. In short, it is the immediacy of audience access afforded by the Internet and Web that contributes so significantly to the attractiveness of do-it-yourself information warfare and terrorism.

PERSONAL INFORMATION WARFARE

Information warfare need not be restricted to group contexts, a fact that is little acknowledged in much of the relevant literature. Ordinary citizens are vulnerable to various kinds of overt and covert attack by cyber-terrorists acting alone or in concert, whether the motivation is ostensibly ludic or demonstrably criminal (Kirsner, 1998; Foote, 1999). Hacker culture may dismiss electronic break-ins and impersonation as punkishly acceptable behaviors (Hafner & Markoff, 1995), but the victim will probably view matters differently. The sense of violation and loss of sanctuary can have long-lasting psychological effects. Some may even question their belief in the First Amendment. To quote Dibbell (1993, p. 41): "The more seriously I took the notion of virtual rape, the less seriously I was able to take the notion of freedom of speech, with its tidy division of the world into the symbolic and the real." Digital media afford one's enemies a much richer and more powerful set of tools with which to engage in psychological warfare, whether at the local or global level. With estimates of e-mail traffic for the year 2000 put at 7 trillion (McHugh, 1998), cyber-smearing or digital defamation campaigns have the potential to reach unprecedentedly large audiences with great speed, in the process creating considerable frustration and collateral damage for the victim (Table 4). The reconstitution of trust and salvaging of reputations in the wake of virtual vilification campaigns will likely pose major challenges for targeted individuals and collectivities.

As with military or business resources, an individual's information assets and online identity are potentially highly degradable by a determined hacker—which isn't to say that

TABLE 4
Digital defamation and virtual vilification

- Ease, swiftness, and stealth of attack
- Overt and covert options
- Target placed on defensive footing
- Extended psychological warfare
- Vulnerability and suggestibility of target
- Cyber-stalking and cyber-smearing
- Ontological warfare possibilities
- Jurisdictional confusion

anything other than a minority of individuals will ever be targeted in systematic fashion by information warriors/terrorists. Think, however, of a university researcher who maintains a large personal Web site containing his or her full curriculum vitae, biographical information, working papers, and survey data sets, as well as personal details. A competent hacker with a grievance against this individual has a number of options to pursue: He or she could systematically corrupt the researcher's data, launch a smear campaign by posting uncorroborated, though superficially plausible, criticisms of the individual's work on a range of listservs, or e-mail members of the relevant academic community with misinformation about the researcher.

The ease with which a "black" public relations campaign can be mounted on the Internet/Web creates appreciable asymmetries in favor of the attacker. The target is thrown on the defensive and left in a state of uncertainty as to the attacker's identity, motives, location, goals, and whether or not the attack is being mounted by an individual or an alliance. Further, the hacker might choose to assume the target's online persona, appropriate his or her personal cyber-identity. Ontological warfare is thus a novel option within the digital battle space, one that makes some postmodernist discussion of rape and identity crises in the context of MUDs and other virtual fora seem tendentious by comparison (Turkle, 1995; Van Gelder, 1995).

CONCLUSIONS

We have tried to show that IW thinking need not be bounded by the discourse of the military community. The principles of information warfare and net terrorism are being instantiated in a diverse set of social contexts, though the range of motivations and practices varies greatly. No longer are cyber-warriors using hit-and-run or scatter-gun assault methods. Instead, they are utilizing well-thought-out tactics and strategies to pinpoint their targets and achieve their objectives in military-like fashion. Playful hacking by a disgruntled graduate student may seem to have little in common with a fundamentalist group's attempt to bring down a commercial jumbo jet by corrupting its on-board computer system, but both actions may be driven by, and exhibit, a common appreciation (conscious or otherwise) of the strategic advantages afforded by information-based modes of attack and retaliation against those whose lifestyles are dependent upon the use of complex information and communication systems. Information warfare not only challenges certain conventional assumptions about the nature of conflict and the potential bases of comparative advantage, but also illustrates some of the hidden properties and paradoxical potentialities (social fusion and fission) of internetworking technologies. It also raises a host of issues about the ethicality of offensive information warfare and the adequacy of existing multilateral codes and conventions to accommodate these new modalities.

Decoupled from their military roots, the language and principles of information warfare have enormously wide applicability. The various facets of information warfare adumbrated here apply with more or less equal plausibility to all four vectors—military, business, social, and personal. Internetworking technologies and the emergence of complex computational communities provide the conditions to support multidimensional information warfare and net terrorism, yet much of the analytic discussion and informed punditry on the social effects of pervasive computing fails to give due acknowledgment to these potentially dystopian effects. Research into the social effects of computing would be greatly enriched by admitting the lexicon of information warfare and information terrorism and by exploring systematically the likely long-term implications of the trends sketched in this article.

REFERENCES

Adams, J. 1998. *The next world war: Computers are the weapons and the front line is everywhere.* New York: Simon & Schuster.

Alger, J. I. 1996. Introduction. In *Information warfare. Cyberterrorism: Protecting your personal security in the electronic age*, ed. W. Schwartau, 2nd ed., pp. 8–14. New York: Thunder's Mouth Press.

Arquila, J., and Ronfeldt, D. 1996. *The advent of netwar*. Washington, DC: RAND.

Bar-Joseph, U., and Sheaffer, Z. 1998. Surprise and its causes in business administration and strategic studies. *International Journal of Intelligence and Counterintelligence* 11(3):331–349.

Boorstein, D. J. 1958. *The colonial experience.* New York: Vintage Press.

Boulanger, A. 1998. Catapults and grappling hooks: The tools and techniques of information warfare. *IBM Systems Journal* 37(1):106–114.

Brophy, P., Craven, J., and Fisher, S. 1998. Extremism and the Internet. Draft final report of the EMAIN project RIC/G/421. CERLIM, Manchester Metropolitan University, Manchester. Available from the authors.

Cronin, B. 1998. Digibabble. *International Journal of Information Management* 18(1):73–74.

Cronin, B., and Crawford, H. 1999. Raising the intelligence stakes: Corporate information warfare and strategic surprise. *Competitive Intelligence Review* 10(3):58–66.

Cusumano, M. A., and Yoffie, D. B. 1998. *Competing on Internet time: Lessons from Netscape and its battle with Microsoft*. New York: Free Press.

De Landa, M. 1991. *War in the age of intelligent machines*. New York: Swerve Press.

Denning, D. E. 1999. Information warfare and security. Reading, MS: Addison-Wesley.

Dibbell, J. 1993. A rape in cyberspace or how an evil clown, a Haitian trickster spirit, two wizards, and a cast of dozens turned a database into a society. *The Village Voice* 21 December:36–42.

Fialka, J. F. 1997. *War by other means: Economic espionage in America*. New York: Norton.

Foote, D. 1999. You could get raped: The inside story of one young woman's terrifying ordeal at the hands of a cyberstalker. *Newsweek* 8 February:64–65.

German, M., Donahue, D. A., and Schnaars, S. P. 1991. A chink in marketing's armor: Strategy above tactics. *Business Horizons* March/April:74–78.

Haffner, K., and Markoff, J. 1995. *Cyberpunk: Outlaws and hackers on the computer frontier*. New York: Touchstone.

Handel, M. I. 1995. Intelligence and the problem of strategic surprise. In *Strategic intelligence: Theory and application*, 2nd ed., eds. D. H. Dearth and R. T. Godden, pp. 213–261. Washington, DC: US Army War College/Defense Intelligence Agency.

Katz, J. 1997. The digital citizen. *Wired* 5(12):68–82, 274–275.

Kirsner, S. 1998. Murder by Internet. *Wired* 6(12):210–216, 266–271.

Libicki, M. C. 1995. *What is information warfare?* Washington, DC: National Defense University, Institute for National Strategic Studies.

McCrohan, K. F. 1998. Competitive intelligence: Preparing for the information war. *Long Range Planning* 31(4):586–593.

McHugh, J. 1998. The old thing behind the next big thing. *Forbes* 30 November:68–74.

Meinel, C. P. 1998. How hackers break in . . . and how they are caught. *Scientific American* October:98–105.

Molander, R. C., Riddile, A. S., and Wilson, P. A. 1996. *Strategic information warfare: A new face of war*. Santa Monica, CA: RAND.

Office of Technology Assessment. 1990. *Critical connections: Communication for the future*. Washington, DC: U.S. Government Printing Office.

Peters, R. 1998. How Saddam won this round. *Newsweek* 30 November:39.

Schwartau, W. 1996. *Information warfare. Cyberterrorism: Protecting your personal security in the electronic age*, 2nd ed., pp. 27–42. New York: Thunder's Mouth Press.

Stoll, C. 1984. *The cuckoo's egg: Tracking a spy through the maze of computer espionage*. New York: Doubleday.

Szafranski, R. 1994. Neo-cortical warfare: The acme of skill? *Military Review* November:41–55.

Szafranski, R. 1996. An information warfare SIIOP. In *Information warfare. Cyberterrorism: Protecting your personal security in the electronic age*, ed. W. Schwartau, 2nd ed., pp. 115–125. New York: Thunder's Mouth Press.

Toffler, A. 1990. *Powershift, knowledge, wealth and violence at the edge of the 21st century*. London: Bantam.

Toffler, A., and Toffler, H. 1993. *War and anti-war: Survival at the dawn of the 21st century*. New York: Little, Brown.

Turkle, S. 1995. *Life on the screen: Identity in the age of the Internet*. New York: Simon & Schuster.

Van Gelder, L. 1995. The strange case of the electronic lover. In *Computerization and controversy: Value conflicts and social choices*, ed., R. Kling, 2nd ed., pp. 533–546. New York: Academic Press.

von Clausewitz, C. 1967. *On war*, eds. M. Howard and P. Paret. Princeton, NJ: Princeton University Press.

Yasin, R. 1998. The enterprise strikes back. *Internet Week* 7 December:1, 78.