*Daniel K. Rosenfield*

# RETHINKING CYBER WAR



ABSTRACT: *Cybernetic attacks have been wrongly perceived as weapons of physical destruction rather than of* disruption. *Because modern, post-industrial societies have become critically dependent on computer networks to function on a day-to-day basis, disruption of those networks could have serious social and economic consequences. In order to better protect society, policymakers will have to re-orient their approach toward cyber security so as to emphasize the genuine cybernetic threat, which is network disruption rather than physical destruction.*

The ongoing debate over cybernetic warfare and the threat it poses to modern society has been overly shaped by a traditional paradigm of warfare. This paradigm emphasizes physical destruction, as opposed to network disruption, as the principal means of inflicting damage on an adversary. While the war-as-destruction framework has been the dominant one since time immemorial, it would be highly misleading to view cyber war within this framework. In fact, it is the disruptive potential of cybernetic attacks, as opposed to their destructive potential, that poses the greatest risk to the security of nations. Cybernetic warfare must be re-evaluated within this new framework in order to be properly understood.

Cybernetic attacks come in two principal forms: those targeting data and those targeting control systems.

Data attacks attempt to steal or corrupt information or deny electronic services to legitimate users of the data. The vast majority of cybernetic

Daniel K. Rosenfield, The George Washington University, Elliott School of International Affairs, 1957 E Street, NW, Suite 301, Washington, DC 20052, thanks Dr. David Alan Grier for reading and commenting on earlier drafts.

*Critical Review* 21(1): 77–90 ISSN 0891-3811 print, 1933-8007 online

DOI: 10.1080/08913810902812156

attacks fall under this category, from online credit-card fraud to Website vandalism to large-scale denial-of-service (DOS) assaults.

Alternatively, control-system attacks attempt to disable or seize control of computer systems governing physical infrastructure such as water supplies, electrical transmission lines, and railroads. The distributed control systems that regulate this infrastructure, such as the SCADA (Supervisory Control and Data Acquisition) systems, have increasingly made use of the Internet to transmit data. For this and other reasons that will be discussed, SCADA systems are potentially vulnerable to hackers (Lemos 2002).

But the cybernetic weapon to fear is the weapon of mass disruption, not mass destruction. There are two reasons for this. First, control-system attacks are extraordinarily difficult to achieve and, even if successful, would not elicit strategically meaningful results. Second, the disruptive potential of cyber war is far more significant than its destructive potential. Advanced, post-industrial societies are now critically dependent on computer networks, and failure or disruption of these networks could have serious social and economic consequences.



## *The Threat from Control-System Attacks*

Information security experts have repeatedly warned of the danger of cybernetic control-system attacks that could target critical infrastructure and result in real-world, physical destruction. For example, an open letter to President Bush in February of 2002 warned that

> our nation is at grave risk of a cyber attack that could devastate the national psyche and economy more broadly than did the September 11th attack. The critical infrastructure of the United States, including electrical power, finance, telecommunications, health care, transportation, water, defense, and the Internet, is highly vulnerable to cyber attack. Fast and resolute mitigating action is needed to avoid national disaster.[1]

The letter was signed by such notables as J. M. McConnell, a former head of the National Security Agency; Stephen J. Lukasik of the Defense Advanced Research Projects Agency; and Sami Saydjari of the Cyber Defense Agency.

The logic behind these fears is compelling. Given the requisite capabilities, cybernetic warfare would be an attractive asymmetric option for adversaries unwilling to array conventional forces against the United States. As Gabriel Weimann (2004) warns:

> The growing dependence of our societies on information technology has created a new form of vulnerability, giving [our enemies] the chance to approach targets that would otherwise be utterly unassailable, such as national defense systems and air traffic control systems. The more technologically developed a country is, the more vulnerable it becomes to cyber attacks against its infrastructure.

The fears expressed by Weimann and others are compounded by the inherent lack of information-security measures protecting automated infrastructure-management systems, such as the SCADA systems. Few if any of these systems were designed with information security in mind because initially, hardly any of them were connected to the Internet. For the most part, these systems were seen as secure from information attacks because of their isolated structure. Today, however, utilities increasingly use the Internet to carry SCADA messages from a growing number of Web-enabled, remote-controlled systems, leaving these systems vulnerable to hacking (Blau 2004). Moreover, critical infrastructure is already a very popular target for computer hackers. A study conducted by one computer-security organization found that in the latter half of 2002, the highest proportion of known computer attacks was directed against critical infrastructure industries such as power and energy (Wilson 2005). Over 80 percent of this infrastructure is privately owned, making it difficult to enforce adequate security protocols (Lemos 2002).

So the perception of danger from cybernetic attacks on critical infrastructure is sound, in principle. But the existing literature on cyber war, along with the historical record, reveals a decidedly different picture. In actuality, the cyber threat to critical infrastructure has been overemphasized at the expense of the more relevant threat of cyber attacks on critical data. The threat posed by control-system attacks is less significant than data attacks because effective control-system attacks are unusually difficult to achieve, and even if successful, are likely to be shallow and transitory in their strategic impact.

## *Fear Not*

The computer networks that manage critical infrastructure are resilient and maze-like. Considerable redundancy is built into these systems, diminishing the potential for attackers to inflict meaningful damage (Lewis 2003). Indeed, experts in the field generally agree that a successful attack would require a great deal of specialized knowledge, typically available only to employees of the managing company (Clark 2001; Dick 2003; Green 2002). Potential cyber assailants would also have to overcome non-computerized fail-safe measures that almost always include human oversight—a virtual impossibility by means of hacking alone (Lemos 2002).

These factors collectively ensure that control-system attacks remain very difficult to pull off, as amply reflected in the historical record: Few control-system attacks are known to have been successful. Furthermore, even when these attacks have succeeded, their consequences have been minimal. For example, one of the few successful attacks ever took place in 1994, when a hacker broke into the computer system governing the Salt River Project, a water facility outside of Phoenix, Arizona. While the hacker clearly trespassed in critical areas, it was determined that he "never could have had control of any dams—leading investigators to conclude that no lives or property were ever threatened" (Lemos 2002). More recently,

> in November 2001, 49-year-old Vitek Boden was sentenced to two years in prison for using the Internet, a wireless radio and stolen control software to release up to 1 million liters of sewage into the river and coastal waters of Maroochydore in Queensland, Australia. Boden, who had been a consultant on the water project, conducted the attack in March 2000 after he was refused a full-time job with the Maroochy Shire government. He had attempted to gain access to the system 45 times, and his last attempt proved successful, allowing him to release raw sewage into the waterways. (Ibid.)

Despite substantial environmental damage, the Queensland incident claimed no lives and cost only $13,000 to clean up; and it required extensive insider knowledge (ibid.).

Control-system attacks simulated by the U.S. government have yielded similar results. In a "digital Pearl Harbor" exercise sponsored by the U.S. Naval War College in July 2002, hackers posing as terrorists were able to simulate a large-scale cyber attack on critical U.S. infrastructure. The results of this exercise indicated that, apart from needing approximately $200 million, high-level intelligence, and five years of preparation, such an attack might cripple communications in some areas but would not result in human deaths or have any other catastrophic physical consequences (Lemos 2002).

In sum, *successful* control-system attacks have been, and are projected to be, extraordinarily rare. (This despite the fact that minor and utterly *unsuccessful* control-system attacks are very frequent, numbering in the thousands every year [Lewis 2003].)

Another reason control-system attacks are difficult to achieve is that cyber defense is not purely a function of computer systems; a significant human element is involved. As Joshua Green (2002) explains, most worst-case scenarios involving control-system attacks presuppose that nobody is monitoring those systems. However, and especially in the case of electrical power grids, oil and gas utilities, and communications companies, the opposite is the case. Furthermore, employees are already well-rehearsed in handling the fallout from disasters such as hurricanes, floods, and tornadoes, and are equally prepared to handle troubles stemming from human action (ibid.). Additionally, infrastructure-management systems are designed to limit the damage from errors and accidents. Manual overrides are commonplace and have been proven to work in response to numerous natural disasters and accidents over the years, from blackouts to telephone-switch failures to disruptions of air-traffic control systems. So while control-system failures might be terribly inconvenient, and engineers might spend days or weeks scrambling to get systems back online, their effects on the general population have been minimal (Schneier 2003).

Air-traffic control systems may provide the best illustration of this. A popular doomsday scenario involves terrorist hackers either seizing control of or disrupting air-traffic control systems and causing airplanes to crash. Again, the human element makes such a scenario highly unlikely. Human operators are constantly monitoring air-traffic control systems, such that in order for disaster to occur, an attacker would have to: (a) compromise the air-traffic control computer system, (b) make sure that air-traffic controllers do not identify the danger right away and react quickly, (c) prevent the controllers from intervening to correct the situation, (d) make sure that the pilots remain unaware of the situation, lest they change flight paths, and (e) "knock down" the many redundancy measures that prevent a situation like this from occurring in the first place (Giacomello 2004).

Even if a major cybernetic attack on a nation's critical infrastructure could be successfully executed, the consequences would likely be shallow and transitory in the physical world. Modern societies deal with failure of critical infrastructure all the time. Blackouts, water outages, air-traffic control disruptions, and telephone-switch failures have been a fact of life since long before the advent of cyber war or even computers. Consequently, industries are well prepared for such contingencies, and the threat of cyber-terrorism has not gone unnoticed by them. The American railroad industry is a prominent example. Federal authorities have long been concerned about the security of computer systems managing the nation's railroad infrastructure. Yet "most rail companies have extensive safety measures and backup systems,"; their "sensors tell when the track has been tampered with, and security mechanisms provide early warning alerts for possible intrusions" (Lemos 2002). The private sector, in this and in many other cases, has recognized the vulnerability inherent in relying on computer networks and has taken steps to prevent or mitigate the problem. The same is true on the consumer end. For instance, even in the event of a successful attack on a metropolitan power grid, many critical systems, such as hospitals and prison operations, would continue running because they have independent generators (ibid.). Because effective disaster preparation is the norm rather than the exception, the military utility of control-system attacks is actually much more limited than what is often assumed.

It should also be remembered that while under certain conditions, control-system attacks could theoretically result in physical destruction, in most cases the damage would be primarily to software systems and therefore not catastrophic. Such attacks would therefore be much easier to recover from than conventional terrorist attacks or strategic air bombardment (for instance). As Kathryn Kerr (2003) explains,

> Recovery from a computer network attack on a critical information system can occur more quickly than a conventional attack—perhaps requiring a reinstall of operating system or other critical applications, back-up files, or additional network hardening etc. By contrast, a conventional attack will usually involve serious physical damage and require the rebuilding of complex pieces of equipment and facilities which is likely to take considerably more time and resources than would be to recover from the system changes due to a cyber attack.

## *The Disruptive Potential of Cyber War*

Far greater military potential lies in the disruptive power of cybernetic attacks than in their destructive power. The more networked a society becomes, the more vulnerable it becomes to disruption. Or, viewed differently, vulnerability is a function of how much wealth is derived from the existence of computer networks. For many countries, ranging from superpowers such as the United States to relatively small yet technologically sophisticated societies like Estonia, both the degree of interconnectedness and the wealth derived from it are considerable. By virtue of this alone, both countries are vulnerable to electronic-network disruption.

Electronic-network disruption would be inflicted through data attacks rather than attacks on computer controls of physical systems. The most dangerous and important form of electronic-network disruption is the denial-of-service (DOS) attack. In a DOS attack, hacker(s) attempt to prevent legitimate users from gaining access to information or services via the Internet. Such an attack could target a computer, its network connection, or the computers and network of a Web site. When successful, DOS attacks keep Internet users from using e-mail, Web sites, online bank accounts, or other services that rely on the affected computer or network. Usually, this occurs when the assailant "floods" a network with information, overloading the server with more requests than it can process. At this point, the server "crashes" and is no longer operable (McDowell 2007).

The disruptive potential of DOS attacks was made clear in mid-2007, when Estonian computer networks were attacked, allegedly by the Russian government. This is the first known instance of a comprehensive cyber attack on a nation-state (Traynor 2007). While the economic damage inflicted on Estonia has not yet been fully assessed, other disruptive cyber phenomena, such as computer worms and viruses, are known to have resulted in billions of dollars of losses. Because their principal effects are the same as those of effective DOS attacks—namely, the disruption of computer networks—they provide a very clear indication of the potential of DOS as an economic weapon. For example, the "SQL slammer" worm, which was activated on January 25, 2003, caused a massive denial of service affecting multiple Internet hosts and roughly 75,000 computers, resulting in an estimated $950 million to $1.2 billion in damage (Dick 2003). The slammer worm "slowed the Internet down to almost a crawl" (ibid.) and raised fears that communication via the Internet might become impossible. The NIMDA worm, discovered in September of 2001, caused an estimated $3 billion in damages and lost productivity (Lemos 2002). Similarly, the ILOVEYOU viruses and its variants were estimated to have affected tens of millions of Internet users and resulted in billions of dollars worth of damages (Denning 2000).

While computer worms and viruses are typically created by individual hackers, a concerted denial-of-service attack perpetrated by a wealthy and capable state might produce much greater disruption. The resulting economic damage could well take place within the context of a widespread disruption of critical government functions, as occurred in Estonia.

Estonia happens to be one of the most wired societies in Europe and has long been a proponent and practitioner of "e-government:" it is highly dependent on computers for both governmental and economic functions. Embroiled in its worst dispute with Russia since the collapse of the Soviet Union, Estonia was subjected to a barrage of DOS attacks in which the Kremlin was implicated with near certainty. The attacks were apparently in retaliation for the decision of Estonian authorities to remove the Bronze Soldier, a Soviet World War II memorial in Tallinn. Russian hackers targeted Websites of the Estonian presidency and parliament; nearly all of the country's government ministries; various political parties; three of the country's six big news organizations; two of the largest banks; and various firms specializing in communications. Though the Estonians were quick to marshal their defenses, mainly by barring access to their Websites from foreign Internet addresses, nearly all of the aforementioned sites were disabled, resulting in severe disruption of government services and economic activity (Traynor 2007).

Other DOS attacks of lesser scale occurred during the 2000 Palestinian *intifada*, with supporters of both Israel and the Palestinians using commonly available attack tools to subvert important Websites and Internet servers. According to one estimate, over 40 hackers from 23 countries participated in the Israeli-Palestinian cyber conflict from October 2000 to January 2001 (Denning 2001). Some 90 or more Israeli websites were reportedly hit in the course of the struggle (Gentile 2000). Another estimate places the total number of websites attacked by both sides at 115, including those affected by DOS attacks, attempts to gain root access, defacements, and a variety of other malicious activities. Targets of data attacks in this conflict included Israeli government sites, financial sites, and Internet Service Providers (ISPs) (Denning 2001). Many additional Websites were indirectly affected and slowed due to the general strain these attacks placed on Net infrastructure in the Middle East. Both sides sustained blows to vital information and financial-resource Websites, such as those of the Palestinian National Authority and the Tel Aviv Stock Exchange (Gentile 2000).

Another DOS attack occurred shortly after the September 11th terrorist attacks, when American hackers retaliated via the Internet. A group of self-labeled "Dispatchers" proclaimed that they would destroy Web servers and Internet access in Afghanistan and other countries that supported terrorism. Led by a 21-year-old Ohioan calling himself "Hackah Jak," the group of roughly sixty hackers defaced hundreds of Websites and launched DOS attacks on the Websites of the Iranian Ministry of Interior and the Presidential Palace of Afghanistan, as well as various Palestinian ISPs (Denning 2001). A more colorful incident occurred during the Kosovo conflict in 1999: When California resident Richard Clark heard of cyber attacks against NATO's Website by Serbian hackers, he decided to send an "e-mail bomb" to the Yugoslav government's Website. A few days later and 500,000 emails into the siege, the site came down. Although Clark did not claim full responsibility for the incident, he admitted that he had "played a part." His Internet service provider, Pacific Bell, subsequently cut off his Internet service, saying that his actions violated their anti-spamming policy (Denning 1999).

DOS attacks, in contrast with control-system attacks, are much easier to achieve given a requisite knowledge of computer systems, and this is reflected in the great number of successful DOS attacks on record. Until the recent cyber attack on Estonia, virtually all of these incidents were small-scale in effect and perpetrated by individuals or small groups of individuals, and their consequences have been negligible in national-security terms. The reason is probably that the perpetrators of the pre-Estonia attacks were nonstate actors, with much more limited technical capabilities than states. Yet as any Estonian defense official will tell you, DOS attacks can be quite effective when directed at the right targets by competent parties. The Estonian cyber attacks, while not yet fully and quantitatively understood in terms of the economic damage they wrought, may be only the first of many to come.

## *Potential Targets for Denial-of-Service / Network Disruption*

The potential targets of disruptive cybernetic attacks can be categorized as either military or economic, although in practice the line between these is somewhat blurred. For example, some reports indicate that, at times, as much as 95 percent of U.S. military traffic is transmitted over civilian communications networks. Significant disruption of these networks could directly affect U.S. military operations,[2] as well as the American economy.

Some experts believe that the U.S. communications infrastructure is highly vulnerable to electronic and even physical attacks due to the critical importance of a few select nodes.[3] Others see the Internet as a whole as the most obvious and probable target of a large-scale DOS attack.

Generally, information-security experts agree that the electronic infrastructure most susceptible to hacking alone is the Internet itself. At least one serious weakness was reported in 1997, "when a technician changed two lines of code and nearly brought down the global network for three hours" (Lemos 2002). According to some, the idea of bringing about a massive failure of the Internet by flooding it with self-replicating transactions, like those that were used against Estonia, "has been already demonstrated on a sufficiently large scale to make such an eventual global threat credible" (Clark 2001).

Dissenting views do exist, however. Steve Cocke, director of the security and stability advisory committee at the Internet Corporation for Assigned Names and Numbers (ICANN), argues that the distributed architecture of the Internet makes it a difficult target to bring down, citing the fact that "when the World Trade Towers came down, local telephone service was severely impaired but disruption of the Internet was minimal" (Blau 2004). And while some national militaries would certainly have the ability to take down the Internet, they are unlikely to do so absent a major great-power struggle. The Internet is far too significant and too useful a part of the world economy.

However, belligerents might try to disable national pieces of the Internet. For example, if Country A went to war with Country B, Country A might attempt to disable Country B's portion of the Internet, or sever connections between Country B's Internet and the rest of the world. Depending on the country in question, low-tech tactics might make this possible, e.g., by disabling the undersea cables used for access. An important question then becomes whether or not Country A's military could turn its own Internet into a domestic-only network if it wanted to (Schneier 2005).

Financial networks, including the websites of stock exchanges and online banking systems, would also be an attractive and feasible target for disruptive cyber attacks. As Giampiero Giacomello (2004) states:

> Institutional investors and financial markets are extremely sensitive to any news that may have even some remote effect on the world economy. Thus, orchestrating a coordinated [cyber] attack that, on the one hand spreads false business information and, on the other, temporarily blocks (e.g., with simple Denial-of-Service) the communications to and from a few major banks or stock exchanges could seriously damage the economies of several advanced countries.

Analysts also stress the importance of "slow-drip mode[s] of attack" that would be harder to detect but more damaging over time—a kind of gradual sapping of an adversary's economy (Kumagai 2001).

Another target particularly appealing to foreign militaries might be U.S. command-and-control systems. The fear that adversaries might successfully subvert command-and-control was brought to the attention of U.S. authorities by Eligible Receiver, the code name for an internal Defense Department exercise in 1997. That year, a group of "red team" hackers from the National Security Agency were able to infiltrate and seize control of the command center computers of the U.S. Pacific Fleet. This was accomplished using only publicly available computer equipment and hacking software.[4] While it is generally agreed that U.S. cyber security has advanced significantly since Eligible Receiver, the exercise continues to be cited as evidence that subversion of command-and-control through information attacks is a very real threat.

The U.S. military, through NATO, has already employed cyber war to disrupt foreign military computer networks, albeit in a very limited fashion. For example, during the 1999 Kosovo war, Coalition forces

> carried out attacks against air defence computers from dedicated jamming aircraft. These attacks marked the first combat use of the specific medium of computer network attack tools by the U.S. military's Information Operations cell. The main thrust of their activities involved manufacturing false radar images and generating signal intelligence intercepts and inserting them into the Serbian air-defence system. Specifically, according to James F. Dunnigan, the U.S. Air Force tapped into Serbian communications networks using satellites and EC 130 Compass Call aircraft in an effort to insert false messages into Serbian systems with respect to non-existent air raids and other attacks. (Davis 2005)

Some believe that the cyber war component to the Kosovo campaign could have been much more significant than it was. Serbian computer systems were extensively interconnected, and this interconnectedness would have allowed for very effective hacking and cyber-war operations, yet NATO chose not to execute a comprehensive cyber attack. The main reason for not acting more aggressively on this front was that NATO lawyers were concerned about the risk of concomitant war-crimes charges if NATO's computer network operations were to cause major damage to civilian infrastructure (ibid.).

From air-defense systems to military wireless networks (Kumagai 2001) to command-and-control and communications systems, cyber war has the potential to seriously disrupt electronic networks and thereby degrade the military capabilities of technologically advanced states. Modern economies that rely extensively on computer networks are particularly vulnerable to disruptive cybernetic attacks. As the case of Estonia indicates, this can have real implications for security and governance. And while they would not inflict any physical damage, data attacks are a far more likely happenstance than control-system attacks, and have the potential to inflict greater social and economic damage.

* * *

The central finding of this analysis is that data attacks are a greater threat to national security than control-system attacks. The latter are unusually difficult to achieve, a fact reflected in the historical record. Few control-system attacks are ever known to have succeeded, despite a very high number of attempts. The difficulty inherent in achieving a successful control-system attack is due to the resiliency and maze-like nature of computer networks managing critical infrastructure, as well as human oversight and built-in mechanical fail-safe measures.

Furthermore, even if a successful control-system attack could be achieved, its political and military utility would be quite limited. Modern societies are well versed in handling the fallout from natural and manmade disasters, and infrastructure attacks historically have failed to coerce enemy populations into surrender. For these reasons, control-system attacks are less of a security risk than commonly thought.

By contrast, data attacks, which can result in cascading failures of information and communications networks, pose a serious threat to the security of modern societies. As computer networks become denser and more integrated worldwide, denial of service is likely to become an even more disruptive and therefore more effective weapon.

Control-system attacks may invoke more visceral fear and garner greater media attention, but denial-of-service attacks are of greater significance to national security.

## NOTES

1. Various authors, letter to President George W. Bush, 27 February 2002. http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/letter.html
2. Interview with a "master hacker." http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/hacker.html
3. Ibid.
4. http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/faqs.html



## REFERENCES


Blau, John. 2004. "The Battle against Cyberterror." *Network World,* 29 November. http://www.networkworld.com/supp/2004/cybercrime/112904terror.html

Clark, Bill. 2001. "The Changed World: An Interview on Cyberterrorism with Paul Strassmann." *BusinessOnline Asia,* Singapore, November. http://www.strassmann.com/pubs/cyberterrorism.html

Davis, Jessica M. 2005. "From Kosovo to Afghanistan: Canada and Information Operations." *Canadian Military Journal,* Autumn. http://www.journal.forces.gc.ca/vo6/no3/informat-01-eng.asp

Denning, Dorothy E. 1999. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." Internet and International Systems: Information Technology and American Foreign Policy Decision-Making Workshop, Nautilus Institute, San Francisco, 10 December. http://www.nautilus.org/gps/info-policy/workshop/papers/denning.html

Denning, Dorothy E. 2000. "Cyberterrorism." Testimony Before the Special Oversight Panel on Terrorism, Committee on Armed Service, U.S. House of Representatives, 23 May. http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

Denning, Dorothy E. 2001. "Is Cyber Terror Next?" *Social Science Research Council* (SSRC.org), 1 November. http://www.ssrc.org/sept11/essays/denning.htm

Dick, Ron. 2003. Interview. "Frontline," PBS, 18 March. http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/dick.html

Gentile, Carmen J. 2000. "Palestinian Crackers Share Bugs." Wired.com, 2 December. http://www.wired.com/politics/law/news/2000/12/40449

Giacomello, Giampiero. 2004. "Bangs for the Buck: A Cost-Benefit Analysis of Cyberterrorism." *Studies in Conflict & Terrorism* 27(5): 387–408.

Green, Joshua. 2002. "The Myth of Cyberterrorism." *The Washington Monthly* (November). http://www.washingtonmonthly.com/features/2001/0211. green.html

Kerr, Kathryn. 2003. "Putting Cyberterrorism Into Context." Auscert.org, 24 October. http://www.auscert.org.au/render.html?cid=2997&it=3552

Kumagai, Jean. 2001. "The Web as Weapon: Will the Networked World Become a New Digital Battleground?" *IEEE Spectrum* (January).

Lemos, Robert. 2002. "What Are the Real Risks of Cyberterrorism?" *ZDNET News.* 26 August. http://news.zdnet.com/2100–1009_22–955293.html

Lewis, James. 2003. Interview. "Frontline," PBS, 18 February. http://www.pbs.org/wgbh/pages/ frontline/shows/cyberwar/interviews/lewis.html

McDowell, Mindi. 2007. "National Cyber Alert System—Cyber Security Tip ST04–015: Understanding Denial-of-Service Attacks." United States Computer Emergency Response Team (US-CERT), 1 August. http://www.us-cert.gov/cas/tips/ST04–015.html

Schneier, Bruce. 2003. "The Risks of Cyberterrorism." *Crypto-Gram Newsletter,* 15 June, Schneier.com. http://www.schneier.com/crypto-gram-0306.html#1

Schneier, Bruce. 2005. "Cyberwar." *Crypto-Gram Newsletter,* 15 January, Schneier.com. http://www.schneier.com/crypto-gram-0306.html#1

Traynor, Ian. 2007. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian,* 17 May. http://www.guardian.co.uk/russia/article/02081438, 00.html

Weimann, Gabriel. 2004. "Cyberterrorism: How Real Is the Threat?" United States Institute of Peace Special Report No. 119, United States Institute of Peace, December. http://www.usip.org/ pubs/specialreports/sr119.html

Wilson, Clay. 2005. "Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress." CRS Report for Congress, Order Code RL32114, 1 April. Congressional Research Service, The Library of Congress.