



---

---

## A Different Kettle of Fish: Computer Network Attack

---

---

Roger W. Barnett

**T**he Information Age has dawned, and it is maturing rapidly. How remarkable the celerity and scope at which the entire world is becoming one far-flung network! As one pundit observed, “To a first approximation, all computers in the world are connected to each other.” Indeed, when one connects to the Internet, he or she is linked globally to all other computers on the Internet. In 1999 there were nearly 200 million Internet users worldwide; by the year 2003, at least another 100 million are expected to be on line.

Some have suggested that, in terms of technological progress, these are revolutionary times. Yet, as long ago as the decade after the orbiting of Sputnik, Soviet authors wrote about a “Revolution in Military Affairs.” The instrument that effected this particular revolution was the marriage of the intercontinental range ballistic missile with the nuclear weapon warhead. This combination meant that, for the first time in history, *strategic* attacks (attacks with the potential to alter the course and outcome of a *war*, as opposed to an attack with the potential to alter the course and outcome of, say, a *battle*, which would be at the *tactical* level) could be conducted at any time against any target in the world. This was genuinely revolutionary, and had to be addressed by developing a wholly new set of concepts, doctrines, and international rules. Today, the close-coupling of societies by information technologies is beginning to portend the same effect—potentially a

strategic effect—but without the necessity for nuclear weapons or long range missilery. Just as the Soviets noticed something revolutionary going on, this is also a major occurrence, but it is also a different kettle of fish.

While the Soviet “Revolution in Military Affairs” offered to produce strategic effects, the means to accomplish this end was centralized in the hands of the State. For good or ill, the power was concentrated, and it was a power that could be acquired only with significant technological effort and at great expense. Today, the potential for a *strategic information systems attack* has become a reality.<sup>1</sup>

What makes this so remarkably different is not only the effects that might be produced without the use of nuclear weapons, but also the diffuse availability of this power. The entry costs to conduct a strategic information attack are insignificant—an inexpensive computer, some easily obtainable software, and a simple connection to the Internet. In theory, anyone just about anywhere can gain access and mount an information attack that might bring about devastating results. Moreover, using this ubiquitous capability, strategic effects might be wrought with little physical damage and no loss of life. Conceivably all national infrastructural components could be vulnerable: telecommunications; food, water, oil, gas, and electrical distribution; health care; education; finance; industry; and also military facilities, networks, command and control, and personnel.

Even more disconcerting, such strategic attacks can be conducted anonymously. Heretofore, the concentrated power of long-range nuclear weapons was in the hands, and under the responsibility and accountability of, governmental officials. Military means, especially those with strategic consequences, were tightly and centrally controlled. Time, technology, and the change in the way in which societies create wealth have changed all that. Thomas Czerwinski has cautioned that “As the ‘combat form’ in any society follows the ‘wealth creation form’ of that society, the wars of the future will be predominantly, but not solely, ‘Information Wars.’ ”<sup>2</sup>

Now nameless, faceless actors can potentially attain strategic objectives; and the possibility exists of not being able to identify the perpetrators and hold them accountable. Because of the diffusion of power, the anonymity and ease of access, the speed at which attacks can be mounted, and the paucity of observable preparation (resulting in little or no warning time), control or regulation of cyberspace attacks, as might be attempted by legal means, seems almost beyond comprehension. Yet, efforts must be made, for the stakes are high.

To ascertain at what points legal instruments might be effective either in preventing attacks or in mitigating their consequences, the ingredients of an attack can be factored into five parts for analysis.

- *Objectives to be sought.* These could range from overturning the ruling political power to the infliction of sheer pain.
- *Actors with motivation.* Motivations might be political, anarchic, criminal, monetary, or merely to vandalize.
- *Inexpensive, easy-to-use tools.* Low expense and ease of attaining powerful tools increase the potential for their use.
- *Access to a variety of targets* almost too numerous to count. A key route of access would be via the Internet.
- *Wide-ranging results,* from mere copying of information (no direct injury from the act) to contaminating the water supply of a large metropolitan area, to sparking economic chaos, to causing the release of a weapon of mass destruction.

Recognizing that these categories are interdependent, it is nevertheless useful to break each of them out for individual discussion.

### Objectives

Access to information empowers. Someone who has the ability to review and change a pay schedule or an academic grade, for example, wields significant power. A person with access to private or classified information can use that information in a variety of ways, not all of which are beneficial or lawful. If the stakes are high enough, the temptation to copy, or alter, or pilfer information can be very strong.

Objectives for obtaining, altering, or obliterating information can vary, depending on the kind of information, its potential uses and value, and the ease in accessing it. Conceivably, governments could be toppled by a malefactor with the right information. The sheer volume of information flow—in the form of e-mail, financial transactions, and telephone calls, for example—means that if only a very small fraction is corrupted, intercepted, or stolen, enormous problems can ensue. Each day over a trillion dollars circulates electronically in the global currency market, and in excess of nine billion e-mail messages are sent in the United States alone. An error, loss, or siphoning rate in the currency market of only one one-hundredth of one percent (.0001) equates to more than \$100,000,000. Numbers (and tolerances) such as these border on the incomprehensible. Consider the potential damage that could be wrought by an unauthorized person changing a bank's financial records by a simple instruction such as "change all sevens to ones." Or even more deviously, change every third seven to a one. Or, perhaps, change the first one thousand sevens to ones, change the

second two thousand fours to twos. Such instructions are trivial for someone with very modest computer literacy to compose, but the difficulty and cost to repair the damage could be significant.

Information has the special property that it can exist in more than one place at one time. This is at the same time an advantage and a disadvantage; for example, decision makers can view and act on the same information simultaneously, even though they are widely separated by distance. On the other hand, it can permit the compromise of valuable or sensitive information without its owner's knowledge.

Information also frequently has an element of timeliness; that is, information can be so perishable that it can have great value at one point in time and be worthless at a later—or conceivably even an earlier—time. Thus, the value of information depends on its availability, its integrity, and its confidentiality.

For those who would seek to attack the information of others, these would be the targets. Availability includes the loss of information, delay in its receipt, and the loss or delay of an information service. Integrity includes unauthorized changes in the information or the introduction of false data. Confidentiality means the unauthorized access to data or information that has some requirement for protection or privacy. In some cases, no damage to the data will result from exploitation. The data might be undisturbed, but its revelation could have severe repercussions.

An additional complication is presented by the medium of "cyberspace." Because cyberspace is viewed as a virtual realm, it carries an aura of unreality. From his bedroom, a young hacker connects to the Internet, travels thousands of miles in seconds, enters the computer system of a large corporation, and views the data contained on storage devices there. His unauthorized presence may or may not be detected. If he destroys data on the storage device, by a mere series of key-strokes on his keyboard, there is no fire, smoke, or noise. The information just disappears. The tactile experience, the physical environment in all its manifestations, the sense of personal danger, and the resultant damage from such an activity are unreal, truly virtual. They are far removed from an actual, corporal breaking and entering, but the transgression is the same.

Have any cyberspace events taken place to the extent that severe consequences, either monetary loss or damage to national security, resulted? To date, there is little evidence to support such a claim, but it is well within the realm of the possible. One might not know whether such attacks have taken place, in part, because if any institution suffers a loss, it has great incentives to suppress that fact. Confidence of investors or customers can be greatly undermined by such a revelation. Moreover, the fact that an institution was attacked and suffered losses can inspire additional attacks on other institutions. But central to the issue of

objectives, one must analyze what gain might accrue to the perpetrator of such acts. If the objective is sheer malice, or to inflict pain with no anticipation of gain, then protection is at the level of maximum difficulty. The same is true of terrorism, for example. If terrorists have an agenda or an objective, one seeks to deter them by withholding the objective. In effect, they are told, "You might be able to injure me, and to inflict great pain on me, but you cannot attain what you seek—so you might as well not even make the attempt." If, on the other hand, terrorists intend only to cause pain and suffering, and they place little or no value on their own lives or prospects, then they become exceedingly difficult to deter.<sup>3</sup>

If, rather than wanton damage, the objective is monetary gain, political change, or competitive advantage, it is helpful for the defender to try to anticipate or envision the objectives of the perpetrator. In that way, the defender can erect active or passive defenses to try to thwart an attack or to minimize or otherwise manage the consequences of a successful attack.

### Actors

Closely coupled to the question of objectives is the issue of actors. In information attack it has become a simple matter for anyone, virtually anywhere, to gain unauthorized access to information. This means, literally, that any modestly literate person who has minimum capabilities in computing can be a participant in information attack or exploitation. From the lowest level (drawing moustaches on billboards or spray painting subway cars) to the highest (gaining unauthorized access to the information held by a large corporation or government), the difference in capability of the actor is remarkably small. This means that children can be recruited and taught the necessary skills; indeed many of the identified "hackers" have been minors.<sup>4</sup> The entry fee, in short, is low in terms of capability, and tends to be low in terms of age as well.

As a special commission reported to the President of the United States:

Like any new tool in previous eras, computers can be used by those who prey on the innocent. International narcotics traffickers now routinely communicate with each other via computer messages. Hostile governments and even some transnational organizations are establishing cyber-warfare efforts, assigned the mission of crippling America's domestic infrastructure through computer attacks. Hackers destroy cyber-property by defacing homepages and maliciously manipulating private information. Pedophiles stalk unsuspecting children in computer chat rooms. Individuals post homepages with instructions to manufacture pipe bombs, chemical weapons, and even biological agents. Crooks

break into business computers, either stealing funds directly or extorting payments from companies anxious to avoid more expensive disruption. Disgruntled employees, with valid access to their companies' system, can take steps to disrupt the business operations or steal proprietary, sensitive, and financial information. And our personal data is at risk of being unlawfully accessed and read by malicious individuals, without our knowledge, as it resides on or traverses communications and computer networks.<sup>5</sup>

No longer is espionage something undertaken exclusively—or, perhaps, even primarily—by professional spies in highly adversarial countries; the field is now open to rank amateurs on a global basis, with or without political, cultural, or religious axes to grind. No longer is sabotage reserved to anarchists, social activists, or well trained enemies of the State; the electronic environment of cyberspace makes it widely available for the doing. Actors may perform their activities in singular privacy, without personal mentoring and a modicum of instruction. Alternatively, they may be organized and scripted by anti-government groups, or as part of a government or industrial team. Accordingly, security forces guarding against electronic attack or exploitation will have great difficulty in “profiling” potential perpetrators.

State-supported acts are in a class of their own. As noted, however, they might well be indistinguishable from mere “hacking.” The non-governmental culture that underwrites computer network attacks (CNA), however, knows no international boundaries, and it tends toward alienation and hostility. Here is an excerpt of the “Hacker’s Manifesto,” in which can be heard echoes of the ravings of the infamous Unabomber:

This is our world now . . . the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt cheap [sic] if it wasn’t run by profiteering gluttons, and you call us criminals. We explore . . . and you call us criminals. We exist without skin color, without nationality, without religious bias . . . and you call us criminals. You build atomic bombs, wage wars, murder, cheat, and lie to us and try to make us believe it is for our own good, yet we’re the criminal. . . . Yes, I am a criminal. My crime is that of curiosity. . . . My crime is that of outsmarting you, something that you will never forgive me for. I am a hacker and this is my manifesto. You may stop this individual, but you can’t stop us all . . . after all, we’re all alike.<sup>6</sup>

Among the most feared and powerful of all actors in attacks on information are insiders. In part, this is because the strength and integrity of a network is

largely a matter of perception. From an outsider's point of view, a network might appear very robust. It has many nodes, many links, many alternatives to routing information, and good security. To an insider who knows the network, there might appear to be a substantial number of vulnerabilities. An outsider is reluctant to attack what seems to him to be a very difficult, very adaptive target. The insider, however, knows the system and its potential weaknesses. This is why the insider is of such high concern—he's inside the firewall, inside the security. His trustworthiness and reliability then ascend to the level of pivotal issues.

Motivation of actors must be viewed as a major variable in the process. For one who acts from the outside, the rewards might be monetary, political, religious, or perhaps just personal satisfaction. For an insider, the motivations might be much less consequential. Changes in workplace environment or relationships, revenge, malicious acts at the behest of an outsider, the challenge, sheer curiosity, or even a misguided good-faith effort to fix a problem can all stimulate an insider to action that could be exceedingly damaging and costly.

Because "cyberspace" has been so ill-defined, because it was initially commandeered by the youth of the world, because it is so easily accessible, and because it is global and instantaneous, almost anyone can become an actor within its confines.

## Tools

On a daily basis, new tools for attacking networks are honed and made available via the Internet to anyone who wants them. Many are free merely for the downloading. According to Bruce Middleton, an expert on the subject, "The most popular of these tools fall into several categories: password crackers, port scanners, war dialers, general network vulnerability scanners, and intrusion detection systems."<sup>7</sup>

Because many firewalls and other security devices require a password to breach them, *password crackers* attempt to determine what the user's password might be. It is a well-known fact that the most widely used password, owing to the fact that employees are lazy and do not understand (or often care about) security, is "PASSWORD." Easy-to-crack passwords involve variations of people's names, their addresses, their pet's names, or the names or nicknames of their favorite sports team. If a match fails on these easy passwords, the password cracker employs a dictionary that very rapidly tries words until the password is discovered. In general, the password cracker can no longer just try each potential word at the locked door (firewall) of the target site, for now most sites can detect such efforts and will not accept password attempts beyond about three. So, some other method must be used, such as locating the password file on the

victim's computer and trying to decrypt it, or catching passwords "on the fly" with a "sniffer."

*Port scanners* "knock on the door" of networks to see if they are unlocked. Many, many computers and services connected to the Internet, for example, have no protection against penetration. Port scanners try to find these unprotected ports and then gain access to information on the victim computer. Many of the "no need to dial up" or "on all the time" services (Integrated Services Digital Network (ISDN) and "Web TV" fall into this category) can place their users in a vulnerable position if they do not include security services. It is the function of port scanners to find those unsecured computers. "Strobe" is an example of such a scanner. It "attempts to locate and build a picture of all ports on one or several hosts in a given network, using what is considered a very efficient algorithm that helps optimize speed. It then displays all those ports that are turned on, or 'listening.'"<sup>8</sup> Strobe is available on the Internet at no cost.<sup>9</sup>

*War dialers* organize banks or networks of modems to dial the same number repeatedly in order to overload it or keep it from receiving other signals, or they might dial many numbers rapidly in the hope of detecting a computer on the other end. These can be very effective in situations where computers are networked but also employ modems to the outside via phone lines. Often computers are manufactured with internal modems installed. Users then merely have to connect their computers to a telephone line, and they can operate in cyberspace outside the firewall that protects the network to which their computers are also attached. Because users can connect to the outside directly, the "outside" can also enter their computers via this route, around the firewall or protective device. War dialers are easy to implement, and can be used with devastating effects on a targeted site.

*General network vulnerability scanners.* Perhaps the most famous of these is SATAN, the Security Administrator's Tool for Analyzing Networks. It has many functions and has been available, also for free, literally for years on the Internet. SATAN analyzes a target computer system and provides the user a detailed report on the kind of equipment, directories, and hosts supported.

*Intrusion detection systems* help secure computer systems. They have a variety of bells and whistles, some of which are detailed record keeping of attempted intrusions, alerts to operators of attacks, and recommended actions to correct the problem or even to respond. In this class one finds ISS SafeSuite, Cisco Net Ranger, NAI CyberCop, and AXENT Technologies NetRecon, to mention only a few.

In addition to these technical tools, there are also "social tools" commonly in use. For example, there is "dumpster diving," where trash is screened for

passwords, file information, personal information, and any other data that might aid a perpetrator's efforts. This is a common procedure; it has been used for years, and it still pays off. Often, armed either with the material gathered from dumpster diving or sheer gall, a potential attacker will then engage in what has become known as "social engineering." For example, a telephone call will be made to an employee in the targeted organization and a misrepresentation made in order to elicit the compromise of protected information. A common ruse is to call an employee and pretend to be an "information management systems troubleshooter." The employee is told that the system is experiencing difficulties, and that the employee's system name and password are needed to fix the problem. For many of the same reasons that "password" has the highest frequency of usage, this technique is very often successful, because it takes advantage of the propensity of people to pay little attention to security.

Peter G. Neumann has summarized quite succinctly the potential for "computer misuse," in the table reproduced below:

Mode	Misuse type
<b>External</b>	
Visual spying	Observing of keystrokes or screens
Misrepresentation	Deceiving operators and users
Physical scavenging	Dumpster-diving for printout
<b>Hardware misuse</b>	
Logical scavenging	Examining discarded/stolen media
Eavesdropping	Intercepting electronic or other data
Interference	Jamming, electronic or otherwise
Physical attack	Damaging or modifying equipment, power
Physical removal	Removing equipment and storage media
<b>Masquerading</b>	
Impersonation	Using false identities external to computer systems
Piggybacking attacks	Usurping communication lines, workstations
Spoofing attacks	Using playback, creating bogus nodes and systems
Network weaving	Masking physical whereabouts or routing

<b>Pest programs</b>	Setting up opportunities for further misuse
Trojan horse attacks	Implanting malicious code, sending letter bombs
Logic bombs	Setting time or event bombs (a form of Trojan horse)
Malevolent worms	Acquiring distributed resources
Virus attacks	Attaching to programs and replicating
<b>Bypasses</b>	Avoiding authentication and authority
Trapdoor attacks	Utilizing existing flaws
Authorization attacks	Password cracking, hacking tokens
<b>Active misuse</b>	Writing, using, with apparent authorization
Basic active misuse	Creating, modifying, using, denying service, entering false or misleading data
Incremental attacks	Using salami attacks
Denials of service	Perpetrating saturation attacks
<b>Passive misuse</b>	Reading, with apparent authorization
Browsing	Making random or selective searches
Interference, aggregation	Exploiting database inferences and traffic analysis
Covert channels	Exploiting covert channels or other data leakage
<b>Inactive misuse</b>	Willfully failing to perform expected duties, or committing errors of omission
<b>Indirect misuse</b>	Preparing for subsequent misuses, as in off-line preencryptive matching, factoring large numbers to obtain private keys, autodialer scanning

Source: Peter G. Neumann, *Computer-Related Risks* (New York: Addison-Wesley Publishing Company, 1995).

## Targets

The variety of objectives, the multiplicity of actors, and the great array of tools together are a clear indicator that the target set is large and rich. Targets range from very specific systems, persons, or infrastructures that are linked tightly with a perpetrator's objectives, to sheer random, serendipitous discoveries. Depending on the motivation of attackers and the tools available to them,

the attack might be precisely focused on a known, discrete target; or it might take the form of a blunt, across-the-board destructive blow to an entire information system. The attacker might use a variety of techniques to gain access, and the effort might take a long time—perhaps spanning months, or even years.

Monetary flows and financial databases, because they offer the prospect of great gain with comparatively low pain or risk, are prime targets. Presumably, the greater the sensitivity or the value of information, the more carefully it will be protected. This is only a presumption, however, because many information systems and vital services were designed, and constructed—and they are operated—with no conception of, or attention to, any threat.

National infrastructures have come under increasingly intense scrutiny in recent years as potential targets for information attack. Because of the growing danger, President Clinton, on July 15, 1996, issued Executive Order 13010 establishing a Presidential Commission for Critical Infrastructure Protection (PCCIP). Chaired by retired Air Force General Robert T. Marsh, the commission identified eight infrastructures that must be protected from the depredations of information and other kinds of attack. These were: electrical power, gas and oil (storage and transportation), telecommunications, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government services. The PCCIP presented the results of its inquiry in October 1997.

Another attractive target is the US Department of Defense. The Deputy Secretary of Defense testified in 1998 that “95 percent of all of our communications now go over public infrastructure—public telephone lines, telephone switches, computer systems, et cetera.”<sup>10</sup> Much of this departmental information is routine and administrative, which is not to say that it is unimportant. Virtually all logistics and medical information on service members travels over the public infrastructure, for example. If antagonists were unaware of such a dependency before, they clearly are now mindful of that vulnerability, and one prudently must assume that they are planning ways to exploit it.

If, indeed, essentially all computers in the world are connected, then that constitutes about as target-rich an environment as can be imagined.

## Results

The horizons being very wide and deep for information operations, and specifically computer network attack, the results also occupy a broad spectrum. From a mere nuisance of defacing a web page with a political message to the loss

of great amounts of money, or potentially lives, the results vary with the objectives, attackers, tools, and targets, as well as the vigor, and the rigor, with which targets are defended.

Exhortations have been raised that the United States is a prime candidate for an “Electronic Pearl Harbor.” Those who issued such a warning meant that the United States is unprepared and not watching very closely, can be surprised, and that the results might well be truly shocking. Of course, beyond the initial trauma, what Pearl Harbor (and the subsequent declarations of war) accomplished was to anger the American public and focus it laser-sharp on conducting war against the Axis powers. Given these facts, some argue that the reason more catastrophic events have not occurred—bringing down the Internet, for example, which some have contended is possible—is that potential attackers fear the “post-Pearl Harbor” backlash.

To date, no catastrophic event has occurred because of computer network attack. Estimates of loss are difficult to make and for that reason often lack credibility. If a particular company is prevented from doing business on the Internet for, say an hour, what is the cost of that? Was a once-in-a-lifetime opportunity missed, with incalculable costs? Opportunity costs are especially difficult to estimate, and that is frequently what is lost in a computer network attack.

So, results could vary from the time lost to clean up the graffiti on a defaced website to, perhaps, billions of dollars in a financial transaction, drug deal, or extortion. National infrastructures could be successfully attacked by CNA, with very disruptive results, and perhaps high innocent loss of life.

The potential to wreak great damage virtually anywhere in the world, almost instantaneously, at very low cost, by almost anyone is imminent. International law offers a prospective tool to attempt to help control or mitigate the potential dangers. Each of the ingredients of an attack listed above offers a possible pressure point for legal application. As analyses and discussions on the subject proceed, these five points can provide a useful framework upon which to build.<sup>11</sup>

---

## Notes

1. Distinctions have been made in the literature of information warfare between data, information, knowledge, and wisdom. This essay deals with tangibles: information is data that has been *organized* or *assessed* in some manner. *Knowledge* and *wisdom* have no independent existence outside the observer. Data and information exist regardless of whether they are known or interpreted.

2. Thomas J. Czerwinski, *The Third Wave: What the Tofflers Never Told You*, 3 STRATEGIC FORUM #72 (1996).

3. For an extended discussion, see Roger W. Barnett, *Information Operations, Deterrence, and the Use of Force*, NAVAL WAR COLLEGE REVIEW, Spring 1998, at 7–19.

4. "Hackers" seek to differentiate between themselves and "crackers." They view the latter as malicious, irresponsible social elements, while they, merely in the interest of science—or perhaps helpfulness—are doing no harm.

5. William Cohen, Janet Reno, William Daley, and Jacob J. Lew, *Preserving America's Privacy and Security in the Next Century: A Strategy for America in Cyberspace*, A Report to the President of the United States, September 16, 1999.

6. Revelation and LOA [Legion of the Apocalypse], *The Ultimate Beginner's Guide to Hacking and Phreaking*, Volume 2, April 1, 1997.

7. Bruce Middleton, *Using the Hacker's Toolbox*, SECURITY MANAGEMENT MAGAZINE, June 1999, [www.securitymanagement.com](http://www.securitymanagement.com).

8. *Id.*

9. According to Middleton, *supra* note 7, most of these free tools can be acquired at: <ftp://coast.cs.purdue.edu/pub/tools>.

10. *Quoted in US Joint Chiefs of Staff, INFORMATION ASSURANCE: LEGAL, REGULATORY, POLICY, AND ORGANIZATIONAL CONSIDERATIONS* 55 (4th ed., 1999) 52.

11. Following is a short list of references on the subject:

JAMES ADAMS, *THE NEXT WORLD WAR: COMPUTERS ARE THE WEAPONS AND THE FRONT LINE IS EVERYWHERE* (1998).

Bruce D. Berkowitz, *Warfare in the Information Age*, ISSUES IN SCIENCE AND TECHNOLOGY, Fall 1995.

JOHN ARQUILLA AND DAVID RONFELDT, *IN ATHENA'S CAMP: PREPARING FOR CONFLICT IN THE INFORMATION AGE*, Santa Monica, CA: RAND, (1997).

RICHARD BRODIE, *VIRUS OF THE MIND: THE NEW SCIENCE OF THE MEME* (1996).

ALAN D. CAMPEN AND DOUGLAS H. DEARTH, *CYBERWAR 2.0: MYTHS, MYSTERIES, AND REALITY* (1998).

DOROTHY E. DENNING, *INFORMATION WARFARE AND SECURITY* (1999).

David J. DiCenso, *IW Cyberlaw: The Legal Issues of Information Warfare*, AIRPOWER JOURNAL, Summer 1999, at 85–102.

LAWRENCE T. GREENBERG, SEYMOUR E. GOODMAN, AND KEVIN J. SOO HOO, *INFORMATION WARFARE AND INTERNATIONAL LAW*, Washington, D.C.: National Defense University, (1997).

MARTIN C. LIBICKI, *WHAT IS INFORMATION WARFARE?* Washington, D.C.: National Defense University, (1995).

WALTER GARY SHARP, SR., *CYBERSPACE AND THE USE OF FORCE* (1999).

MARK RUSSELL SHULMAN, *LEGAL CONSTRAINTS ON INFORMATION WARFARE*, Occasional Paper No. 7, Maxwell Air Force Base, AL: Air University, 1999.

DON TAPSCOTT, *GROWING UP DIGITAL: THE RISE OF THE NET GENERATION* (1998).

Chairman of the Joint Chiefs of Staff, *Joint Publication 3-13, Joint Doctrine for Information Operations*, (1998).

Internet sites:

[www.infowar.com](http://www.infowar.com)

[www.terrorism.com/infowar/index.html](http://www.terrorism.com/infowar/index.html)

[www.cert.org/](http://www.cert.org/)

[www.twurled-world.com/Infowar/Update2/cover.htm](http://www.twurled-world.com/Infowar/Update2/cover.htm)

[www.antonline.com](http://www.antonline.com)

[www.ita.org](http://www.ita.org)