

# Computer Crime

Richard C. Hollinger, Ph.D.  
University of Florida, Gainesville, FL

The first Electronic Numerical Integrator and Computer (ENIAC) was switched on over 50 years ago in February of 1946. While the beneficial contributions of new technologies are usually the first to be noticed, oftentimes the negative ramifications become apparent only much later. This was not the case with the computer, as cases of computer abuse began to be documented from the outset (Parker 1976; Wasik 1991).

By the late 1970s "crime by computer" was a serious enough problem to merit new criminal statutes prohibiting a wide range of acts previously not covered by existing law (Hollinger and Lanza-Kaduce 1988). Today, each of the 50 United States and the federal government has criminalized unauthorized system access, software piracy, theft of computer services, and the alteration or theft of electronically-stored information. Similar laws have been passed recently in Australia, Canada, France, Germany, Holland, Singapore, the United Kingdom, and most other technologically advanced countries around the world (Cove, Seger, and VonStorch 1995).

## FOUR FOCAL PERIODS

The phenomena of crime by computer can be divided into four distinct focal periods (Hollinger 1997). The first interval can be called the discovery period. Roughly between 1946 and 1976, the focus of attention was on describing the computer abuse phenomenon. The second period can be characterized as the criminalization period. The principal activity during this period (1977 to 1988) was concentrated on "correcting" numerous deficiencies in the criminal law. The third period revolved around the demonization of the hacker. This 5-year period was characterized by an intensive law enforcement effort to identify, apprehend, and sanction those who are often pejoratively referred to as "hackers" and "crackers." The fourth period, which we are presently in, can be labeled the censorship period. As a result of the explosive growth of the Internet, the current focus of attention has been directed toward limiting the

access of computer users to various "dangerous" materials currently available on the WEB, such as, collections of sexually explicit writings, pornographic pictures, and information on violence and terrorism.

## PERIOD ONE: THE DISCOVERY OF COMPUTER ABUSE (1946-76)

One of the earliest people to write about computer crime was a Stanford Research Institute (SRI) scientist named Donn Parker. While Parker was not the only person to document the phenomenon of computer crime (Bequai 1978), he was the first to become nationally recognized as an expert regarding computer security. Parker collected media accounts of what he called "computer abuse." His somewhat unsystematic collection of news clippings culminated in *Crime by Computer* (1976). Parker's book quickly became a landmark reference work on the subject.

Since *Crime by Computer* was published before the introduction of the personal computer, virtually all of the examples of computer abuse were acts against mainframe systems. Subsequently, microcomputers and modems became available to the general public in the early 1980s. As a result, the potential for both benefit and abuse from this new technology changed markedly. The inventors of the first personal computers envisioned that personal computers (PCs) would have a revolutionary impact on society, providing access to massive amounts of information regardless of one's social status (Parker 1983).

In the early days of the computer revolution, computer aficionados banded together informally in clubs (e.g., the Homebrew Computer Club in California) to share information and solve technological problems. These first computer users referred to each other as "hackers," reflecting the cooperative and collaborative atmosphere in the early days of computer programming (Levy 1984:23-4). Many different persons would typically "hack" at a string of code before it would run without errors. As such, "hacker," was originally intended as a complimentary recognition of one's computer skills.

However, now the expression is widely used as a derogatory term synonymous with deviant computer use (Hollinger 1991).

The paradoxical struggle between the benefits that computers could bring to society contrasted with the potential for serious abuse soon presented a dilemma to the embryonic computer industry. On the one hand, if computers were made too secure, neophyte users could not easily learn how to use them. On the other hand, if computer systems were not adequately protected from unauthorized users, abuse of the technology was almost invited. The two contradictory objectives of "user friendliness" and "information security" are still problematic (Johnson, 1994).

#### Types of Computer-related Offenses

Since the earliest days of the computer revolution, a wide array of abuse, deviance, and unauthorized activity has been documented. In an effort to categorize the myriad of incidents reported in the mass media, Donn Parker (1976:12-22) concluded that the computer played four distinct roles.

Some of the very first instances of computer abuse were cases in which the machine was the object of the deviance. Computers have been shot, blown up, burned, vandalized, destroyed, and stolen. Another group of abusers employed computers as the instrument with which to perpetrate crimes. For example, instead of using a gun to rob a bank, these enterprising offenders utilized a computer terminal to transfer money or financial assets out of someone else's account into theirs.

Still other computer deviants have employed the symbolic role of the computer by defrauding unsuspecting victims. Because so many people believe without question what they read on computer printout, they unfortunately assume that all computer generated information is completely accurate. A number of fraudulent invoice and false billing scams have been perpetrated in this way.

Each of the above three computer abuse roles is not really a new category of criminal behavior. Most are simply older scams retooled for the computer age. However, there is one new role that the computer can play that is unique. It involves the electronic subject-matter contained in digital forms of storage media. Never before in history has information been stored in a digital medium that can be altered, copied, and deleted without leaving any physical trace. In fact, it is now possible to make exact replicas of digitally-stored intellectual property without any deterioration in the quality or changing the physical location of the original.

#### How Much Computer Crime Occurs?

Given the secretive and hidden nature of computer crime, how much computer criminality is perpetrated

annually? Little is known about the incidence and prevalence of computer-related deviance and crime because very few cases have come to the attention of law enforcement authorities, and even fewer are criminally prosecuted (Conly 1989; Forcht, Thomas and Wigginton 1989; Rosenblatt 1990). Given the paucity of official or reliable data on the subject, researchers have used alternative data sources to estimate the baseline levels. A study in which college students were asked to self-report their involvement in software piracy and unauthorized account access conducted in 1992 found that slightly over 11 percent indicated they had engaged in at least one of these activities during the previous 15-week semester. More specifically, 10 percent had traded software and 3.3 percent had gained unauthorized access to another user's computer account or files (Hollinger 1993). A more recent study conducted among college students at a different university found that over forty percent (41.3 percent) admitted to giving or receiving pirated software—33.9 percent in the past year. Two percent reported that they had written a logic bomb or purposely given someone else a computer virus (Skinner and Fream 1997).

Other studies have noted a gradual process of increasingly more deviant involvement as the computer user becomes more sophisticated in skill. Computer deviants first engage in software piracy, a smaller number graduate into systems browsing, followed by an even smaller number of those who eventually become malicious system "crackers" (Hollinger 1988). Most would agree that software piracy is the most prevalent form of computer-related abuse. The first computer programmers freely shared their own program code with other aficionados (Levy 1984). This altruistic world was soon changed by those who realized that great sums of money could be made from selling, rather than sharing, computer software. Protecting intellectual property from those who would reproduce it without paying or honoring the copyright has become the nemesis of the software industry. Moreover, as little as electronic property ownership is respected in this country, it is even less appreciated in non-Western cultures (Swinyard et al. 1990).

Prior to the passage of the first federal computer crime act (U.S. Public Law 98-473 1984), the American Bar Association (ABA) released a survey of corporate computer users from which it was estimated that at least 25 percent of U.S. firms uncover one or more verifiable incidents of serious computer abuse each year. Collectively the victimized firms reported annual losses that ranged on average from \$2 million to \$10 million (American Bar Association 1984). Other studies have placed the dollar impact of computer hackers and thieves in the United States at somewhere between \$145 million and \$5 billion annually (McEwen, Fester, and Nugent 1989). The ABA study also found that the majority of these victimizations (77 percent), were per-

## 78 Volume II: Crime and Juvenile Delinquency

peretrated not by teenage hackers, but rather by the corporation's own employees.

During 1986, a survey of Forbes 500 corporations was produced by the faculty at Mercy College. This survey indicated that 56 percent of the respondents experienced losses attributable to computer crime in the past year (1984-85). The average loss per incident was \$118,932. As in the ABA study, most of the perpetrators (63 percent) in the Mercy College study were thought to be employees of the victimized firm. Perhaps this explains why more than half of the firms which experienced victimizations did not report the incidents to law enforcement (O'Donoghue 1986).

A statewide survey conducted by the Florida Department of Law Enforcement in 1988 reported that one business in four (24.2 percent) had experienced a known and verifiable computer crime during the past year. Interestingly, at least half (50 percent to 84 percent) of these computer offenders were adult employees of the victimized firm, not school-age hackers. Sixty-five percent of victimized businesses elected not to report any computer crime incidents to law enforcement authorities. In fact, the Florida survey indicated that despite the nation's oldest computer crime statute, two-thirds of the law enforcement agencies surveyed had not investigated a single computer crime during the past year (Herig 1989).

At least three conclusions can be drawn from the results of these studies. First, by the early 1980s computer-related victimizations were occurring with regularity in a small but significant number of businesses and organizations each year, some resulting in large-scale monetary losses (Clough and Mungo 1992). Second, approximately three-fourths of computer crimes were perpetrated by adult employees—not teenage hackers. Finally, the vast majority of computer crime incidents were not referred to the criminal justice system for prosecution (Pfuhl 1987).

### PERIOD TWO: THE CRIMINALIZATION OF DEVIAN'T COMPUTER USE (1977-87)

The first computer crime statute was enacted in the state of Florida during 1978 in response to an ingenious computer fraud perpetrated the year before at the Flagler Dog Track in Hialeah. Many other states soon followed with their own specialized statutes. The impetus to pass state computer crime laws was propelled along by a handful of moral reformers (Hollinger and Lanza-Kaduce 1988). Although few real crimes were being perpetrated, the prospect that a teenage computer hacker could accidentally trigger World War III became the story line which made the 1983 movie, *War Games*, a major box office smash. Ironically, in the very same summer, a group of Milwaukee teens calling themselves the "414 Hackers" broke into scores of computers all across North Amer-

ica. Fiction soon became reality. Within five years virtually all of the remaining states, as well as the U.S. government, passed computer crime laws. The major western democracies also joined in the moral panic enacting a variety of their own computer crime laws during this period. Clearly there were legal issues introduced by this new form of electronic property that current laws could not adequately handle, such as the requirement of asportation (physical movement) to prove a larceny. However, despite very little evidence that a computer crime wave was actually occurring, the fears about what could happen caused few to question whether a new set of laws was really necessary. Most legislators were convinced that computer crime was substantially different from other forms of larceny, theft and trespass (Michalowski and Pfuhl 1991).

### PERIOD THREE: THE DEMONIZATION OF HACKERS (1988-1992)

Years after the passage of a variety of computer crime statutes, few offenders were being prosecuted. Those criminally charged typically were disgruntled employees seeking revenge against their current or previous employers (Herig 1989). The real threat of computer crime has always been from these organizational insiders. Nevertheless, computer security professionals have always been most afraid that a malicious outsider would gain unauthorized access to a critically important computer system—stealing, damaging, or destroying information and programs. Although the risk was always there, by the late 1980s the general public did not yet perceive computer crime as a serious social problem. Some argued that not until a series of "cautionary tales" developed would computer abuse be taken seriously (Williams et al. 1989).

#### *The Internet Worm*

In November of 1988 fears about a large scale threat to the Internet became realized when a brilliant graduate student at Cornell University named Robert T. Morris, Jr., unleashed a "worm" on the worldwide telecommunication network (Spafford 1989). While no real lasting harm was done or intended, the Internet ground to a halt in a matter of hours. Ironically, the young man responsible for the Internet worm, and one of the first persons criminally prosecuted using the newly enacted federal computer crime statute, was none other than the son of the nation's foremost computer security expert (Hafner and Markoff 1991).

#### *The Hannover Hackers*

A number of other computer abuse cases caused concern about the security of the nation's military and corporate computers. In Berkeley, CA, a Lawrence Liv-

ermore Labs research assistant named Cliff Stoll discovered minor discrepancies in the computer accounts at his facility. Stoll (1989) traced the source to a group of German teenagers who were browsing American military computer networks in the hopes of finding defense secrets which they could sell to the KGB. Although they never got access to any classified documents, the mere fact that intruders from a foreign country succeeded in accessing military computers bolstered those who believed that hackers posed a threat to the nation's security.

#### Kevin Mitnick: The "Dark Side Hacker"

Long before the invention of the personal computer, telephone companies had become the targets of vandalism and abuse. Those who figured out how to circumvent the billing system to make free phone calls around the world were called phone "phreaks" (Bowcott and Hamilton 1990). One of the very best of this new breed of telephone company hackers was Kevin Mitnick. After breaking into telephone company offices to steal documentation and spending many hours "dumpster diving" for old printout, Mitnick soon developed a reputation for knowing more about the Pacific Telephone Company's computer system than even their best programmers. Using his expertise, Mitnick perpetrated a series of daring computer crimes, including the downloading of yet unreleased Digital Equipment Company system software from the company's own mainframe. Detected, arrested, but never seriously punished, Mitnick became known as the "dark side hacker" (Hafner and Markoff 1991).

After a girlfriend turned him in, Kevin Mitnick was arrested, sentenced and finally served some prison time. Not to be deterred by those he had learned to loathe, in 1992 Mitnick violated his parole, changed identity, moved, and evaded law enforcement until 1995. He was eventually apprehended in his Raleigh, NC, apartment as the result of detective work conducted largely by Mitnick's last victim, University of California, San Diego computer system manager, Tsutomu Shimomura. Using a laptop, modem, and a cellular telephone, Mitnick had been cracking, browsing, and stealing software, data files, and e-mail from a number of corporate computer systems and Internet providers for over three years (Shimomura and Markoff 1996).

#### Atlanta's Legion of Doom and the E911 System

The law enforcement community was having a hard time mobilizing public support for a massive crackdown on the hacker community. This indifference changed when hackers became interested in the E911 system that most communities use to dispatch police, fire, and emergency services. If some hacker could crash or disable emergency 911 services, there was the

chance that someone might die as a result. The workings of the E911 system were a poorly held secret in the telephone company. In fact, during September of 1988 three members of an Atlanta group calling themselves the Legion of Doom broke into a BellSouth computer and downloaded a document explaining the inner workings of the E911 system. The three Legion of Doom members circulated the document to their friends and even posted it on a computer bulletin board. Recognizing its importance, another subscriber of the bulletin board electronically transferred a copy of the BellSouth E911 document to a University of Missouri student named Craig Neidorf. Neidorf eventually published the document in the February 25, 1989 edition of his electronic newsletter entitled, *Pbrack*. With a guilty verdict all but assured, the prosecutor, William Cook, suddenly dropped all charges in the middle of Neidorf's trial when testimony revealed that the documents alleged to have been stolen were available for sale to the public at the telephone company (Godwin 1994). Despite the unsuccessful result, the Neidorf prosecution had a chilling effect on those concerned about constitutional protections afforded the press (Denning 1991).

#### Operation Sun Devil

Other law enforcement investigations designed to control computer crime have continued to raise serious questions about the actual seriousness of the computer crime danger. Directing a combined task force called Operation Sun Devil, U.S. Attorney William Cook and Arizona Assistant Attorney General Gail Thackeray coordinated a multistate and federal seizure during May 7-9, 1990 of 42 bulletin boards. Ostensibly designed to eliminate most of the rogue bulletin boards, especially those thought to be trading in stolen long distance telephone access codes and credit card numbers, the net result of the "great hacker crackdown" was to discredit the U.S. Secret Service and other participating law enforcement agencies due to a number of serious civil liberty and privacy violations (Sterling 1992).

#### PERIOD FOUR: THE CENSORSHIP PERIOD (1993-PRESENT)

An underlying theme in most computer crime cases of the early 1990s involved the censorship of information and images over private computer bulletin boards and the Internet. While the information superhighway has always been viewed by its users as a source of beneficial information, many in law enforcement worried that it could be put to criminal purposes. Some of the earliest concerns about the abuse potential involved the threat of property crimes being perpetrated (or facilitated) via computer. Stolen credit card numbers were commonly posted on computer bulletins. Tele-

80 *Volume II: Crime and Juvenile Delinquency*

phone long distance providers were fearful that long distance telephone numbers were being shared with thousands around the globe.

#### Pornography and Pedophiles

Telephone and credit card fraud were not the only forms of crime facilitated by a computer connected to a modem. Since it was now possible to telephonically link to thousands of users over the same network, many people began to be attracted to this new method of interpersonal exchange. However, what was fundamentally different about this new form of communication was the anonymity afforded by the computer keyboard. Instead of talking directly to another person, digital messages were typed on the keyboard either in real time (chat rooms) or to be read later (E-mail). Like a computer version of the CB radio, users could say things to each other that they might never express face-to-face. For those who enjoy fantasy relationships, these computer forums provided an extraordinary latitude of expression (Durkin and Bryant 1995).

As one sits at a computer, it is virtually impossible to determine another user's age or gender. As a result of this anonymity, many people interested in sexually-related relationships began to use the various bulletin board systems to foster electronic relationships, and in some cases, in-person meetings (Lamb 1997). For some, these contacts made via computer lead to lasting, mature relationships. However, a small number of adults, especially pedophiles, used the computer to set up meetings with juveniles for the purpose of having sex. Law enforcement agents started to employ sting operations in order to arrest adults soliciting sex from juveniles. These sting operations have led to numerous arrests in virtually every state (Charney 1994). Another creative use of the Internet involved the dissemination of pornography. Pictures of all types could be digitized and distributed via computer. Many digital pictures are not controversial. However, some significant proportion of downloadable images posted on Internet newsgroups are of naked bodies, adults having sex with adults, people having sex with animals, and most controversial, adults having sex with children. Many of these pictures are available via adults-only bulletin boards that require advance registration and membership fees. Nevertheless, because the 1973 Supreme Court decision, *Miller v. California*, ruled that obscenity definitions can be based on local community standards, some bulletin board operators with pornographic material on their systems were arrested. In the most famous case yet two Milpitas, CA, bulletin board owners, Robert and Carleen Thomas, were successfully prosecuted in Memphis, TN, for providing pornographic digital images and selling videos which included pictures of nude children on their system (Wallace and Mangano 1996).

#### Censorship

The mere presence of pornography on the Internet, especially images of children, has prompted the U.S. Congress to prohibit computer pornography. Supported by the powerful Christian fundamentalist lobby, the Communications Decency Act of 1995 (CDA) was the culmination of this censorship crusade. The CDA made it illegal to transmit any indecent message or picture over the Internet that could be seen by a minor. In 1997 the Supreme Court ruled the Communications Decency Act was an unconstitutional assault on the First Amendment.

Not deterred in its war against "cybersmut," Congress recently passed the "Online Child Protection Act." However, in February of 1999 a Philadelphia federal judge blocked implementation of the new law (Cohen 1999). Other courts are currently being asked to rule on the constitutionality of website content and the use of "screening" software placed on the Internet browsers of public library computers. Similar computer censorship battles are being fought in Germany, France, and Australia.

There is no doubt that pornographic images exist on the Internet. The question is what, if anything, to do about it. As "conclusive proof" of the scope of the computer pornography problem, an article was published in the prestigious *Georgetown University Law Review* authored by a Carnegie Mellon University student named Martin Rimm (1995). The Rimm study was purported to be an exhaustive empirical assessment of the contents of the various newsgroups on the Internet and World Wide Web. The conclusion of the Rimm study, namely, that over 80 percent of the files posted on the information superhighway are pornographic in nature, was extremely well received by those on the religious right who strongly support efforts at digital censorship. However, many civil libertarians have alleged that the Rimm study is so biased that it must have been requisitioned by the conservative religious right to justify a need for the proposed censorship legislation (Branscomb 1995). Additional efforts are underway to prevent private citizens from having access to digital encryption software (e.g., Zimmerman's P.G.P.) once formally restricted to use only by the government (Foremski 1992). Undoubtedly, more censorship battles are destined to end up in the courts before these important free speech questions are resolved.

#### REFERENCES

- American Bar Association. 1984. *Report on Computer Crime*. Task Force on Computer Crime, Section of Criminal Justice (June), Chicago, IL.
- Bequai, August. 1978. *Computer Crime*. Lexington, MA: Lexington Books.
- Bowcott, Owen and Sally Hamilton. 1990. *Beating the System: Hackers, Phreakers, and Electronic Spies*. London: Bloomsbury Publishing.

- Branscomb, Anne W. 1995. "Internet Babylon? Does the Carnegie Mellon Study of Pornography on the Information Superhighway Reveal a Threat to the Stability of Society?" *The Georgetown Law Journal* 83:1935-57.
- Charney, Scott. 1994. "Computer Crime." *Federal Bar News & Journal* 41:489-494.
- Clough, Bryan and Paul Mungo. 1992. *Approaching Zero: The Extraordinary Underworld of Hackers, Phreakers, Virus Writers & Keyboard Criminals*. New York: Random House.
- Cohen, Adam. 1999. "Cyberspeech on trial." *Time* 153:52.
- Conly, Catherine H. 1989. *Organizing for Computer Crime Investigation and Prosecution*. Washington, DC: National Institute of Justice.
- Denning, Dorothy E. 1991. "The United States vs. Craig Neidorf: A Debate on Electronic Publishing, Constitutional Rights and Hacking." *Communications of the ACM* 34:22-43.
- Durkin, Keith F. and Clifton D. Bryant. 1995. "Log on to sex: Some notes on the carnal computer and erotic cyberspace as an emerging research frontier." *Deviant Behavior* 16:179-200.
- Forcht, Karen A., Daphne Thomas, and Karen Wigginton. 1989. "Computer Crime: Assessing the Lawyer's Perspective." *Journal of Business Ethics* 8:243-251.
- Foremski, Tom. 1992. "Computer Crime, United States Laws and Law Enforcement." *International Yearbook of Law, Computers and Technology* 6:121-127.
- Godwin, Mike. 1994. "When Copying Isn't Theft: How the Government Stumbled in a "Hacker" Case." *Internet World* (Jan./Feb.), available online at: [http://www.eff.org/pub/Publications/Mike\\_Godwin/phrack\\_riggs\\_neidorf\\_godwin](http://www.eff.org/pub/Publications/Mike_Godwin/phrack_riggs_neidorf_godwin). Article.
- Hafner, Katie and John Markoff. 1991. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster.
- Herig, Jeffrey A. 1989. *Computer Crime in Florida: 1989*. Tallahassee, FL: Florida Department of Law Enforcement.
- Hollinger, Richard C. 1988. "Evidence that Computer Crime Follows as Gutman-Like Progression." *Sociology and Social Research* 72:199-200.
- . 1991. "Hackers: Computer Heroes or Electronic Highwaymen." *Computers and Society* 21:6-17.
- . 1993. "Crime by Computer: Correlates of Software Piracy and Unauthorized Account Access." *Security Journal* 4:2-12.
- . 1997. *Crime, Deviance and the Computer*. Aldershot, England: Dartmouth.
- Hollinger, Richard C. and Lonn Lanza-Kaduce. 1988. "The Process of Criminalization: The Case of Computer Crime Laws." *Criminology* 26:101-126.
- Icove, David, Karl Seger and William VonStorch. 1995. *Computer Crime: A Crime Fighter's Handbook*. Sebastapol, CA: O'Reilly & Associates.
- Johnson, Deborah G. 1994. *Computer Ethics*, 2nd ed. Englewood Cliffs, NJ: Prentice-Hall.
- Lamb, Michael. 1997. "Cybersex: Research Notes on the Characteristics of the Visitors to Online Chat Rooms." *Deviant Behavior: An Interdisciplinary Journal* 19:121-135.
- Levy, Steven. 1984. *Hackers: Heroes of the Computer Revolution*. New York: Doubleday.
- McEwen, J. Thomas, Denis Fester and Hugh Nugent. 1989. *Dedicated Computer Crime Units*. Washington, DC: National Institute of Justice.
- Michalowski, Raymond J. and Erwin H. Pfuhl. 1991. "Technology, Property, and Law: The Case of Computer Crime." *Crime, Law and Social Change* 15:255-275.
- O'Donoghue, Joseph. 1986. *The 1986 Mercy College Report on Computer Crime in the Forbes 500 Corporations: The Strategies of Containment*. Dobbs Ferry, NY: Mercy College.
- Parker, Donn B. 1976. *Crime By Computer*. New York: Charles Scribner's Sons.
- Pfuhl, Edwin H., Jr. 1987. "Computer Abuse: Problems of Instrumental Control." *Deviant Behavior* 8:113-130.
- Rimm, Marty. 1995. "Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories, and Animations Downloaded 8.5 Million Times by Consumers in Over 2000 Cities in Forty Countries, Provinces, and Territories." *The Georgetown Law Journal* 83:1849-1934.
- Rosenblatt, Kenneth. 1990. "Deterring Computer Crime." *Technology Review* 93:34-40.
- Shimomura, Tsutomu and John Markoff. 1996. *Take-Down*. New York: Hyperion.
- Skinner, William F. and Anne M. Fream. 1997. "A Social Learning Theory Analysis of Computer Crime among College Students." *Journal of Research in Crime and Delinquency* 34:495-518.
- Spafford, Eugene H. 1989. "The Internet Worm: Crisis and Aftermath." *Communications of the ACM* 32:678-687.
- Sterling, Bruce. 1992. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York: Bantam Books.
- Stoll, Clifford. 1989. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. New York: Doubleday.
- Swinyard, William R. Heikki Rinne, and Ah Keng Kau. 1990. "The Morality of Software Piracy: A Cross-Cultural Analysis." *Journal of Business Ethics* 9:655-664.
- Wallace, Jonathan and Mark Mangan. 1996. *Sex, Law, and Cyberspace*. New York: Henry Holt.
- Wasik, Martin. 1991. *Crime and the Computer*. New York: Oxford University Press.
- Williams, Mary B., David Ermann and Glaudio Gutierrez. 1989. "Cautionary Tales and the Impacts of Computers on Society." *Computers & Society* 19:23-31.