FBI Law Enforcement Bulletin

July 1995
Volume 64
Number 7

United States
Department of Justice
Federal Bureau of
Investigation
Washington, DC 20535

Louis J. Freeh
Director

The *FBI Law Enforcement Bulletin* (ISSN-0014-5688) is published monthly by the Federal Bureau of Investigation, 10th and Pennsylvania Avenue, N.W., Washington, D.C. 20535. Second-Class postage paid at Washington, D.C., and additional mailing offices. Postmaster: Send address changes to *FBI Law Enforcement Bulletin*, Federal Bureau of Investigation, FBI Academy, Quantico, VA 22135.

Editor
Stephen D. Gladis, Ph.D.
Managing Editor
Kathryn E. Sulewski
Art Director
John E. Ott
Associate Editors
Andrew DiRosa
Julie R. Linkins
Kimberly J. Waggoner
Assistant Art Director
Brian K. Parnell
Staff Assistant
Stephanie L. Lowe

Internet Address:
fbileb@justice.usdoj.gov

Cover photo
© The Image Bank

Features

Focus on Technology

Departments

ISSN 0014-5688 USPS 383-310

156176

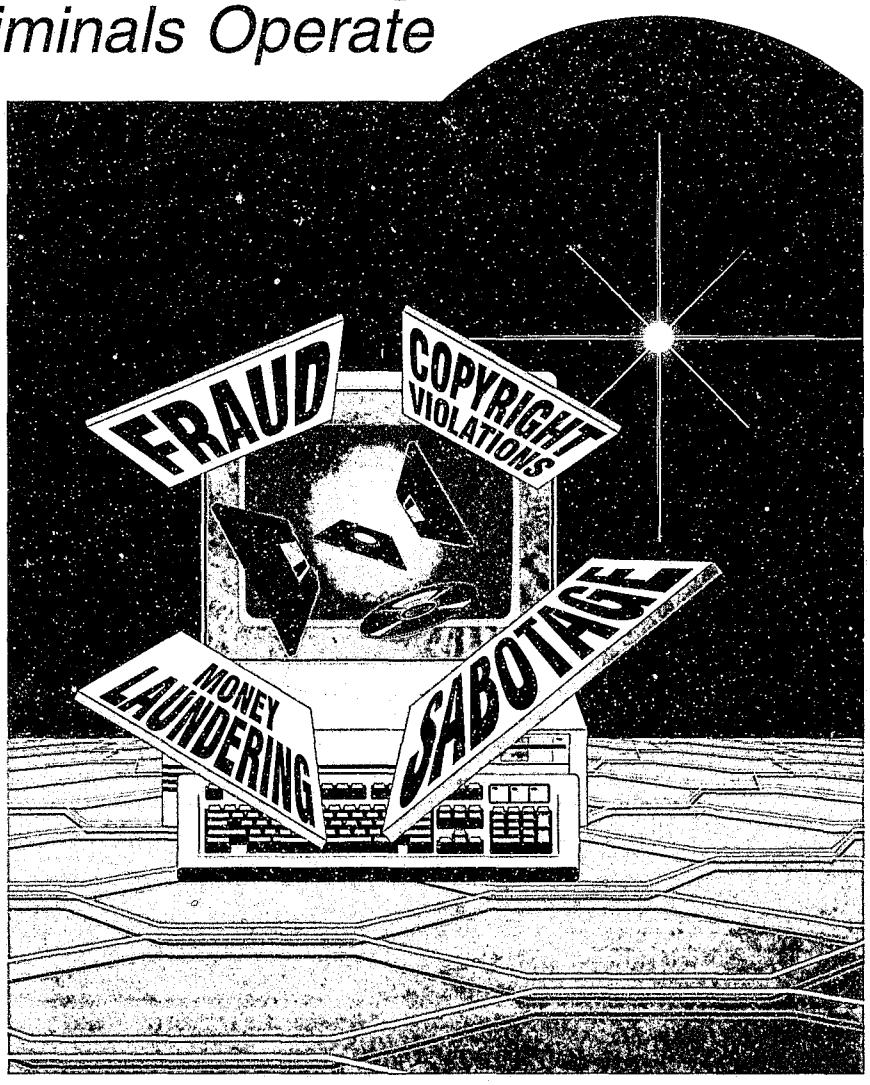
Computer Crime Categories

How Techno-criminals Operate

By DAVID L. CARTER, Ph.D.

"The world isn't run by weapons anymore, or energy, or money. It's run by ones and zeros—little bits of data—it's all electrons....There's a war out there, a world war. It's not about who has the most bullets. It's about who controls the information—what we see and hear, how we work, what we think. It's all about information."

Lines from the character "Cosmos," in the movie *Sneakers*, MCA/Universal Pictures, 1992.



The motion picture *Sneakers* focused on computerized information as a valuable commodity and on the technological means to invade and steal that commodity. To many, the high-tech wizardry of the movie probably appears exotic; however, it is much more realistic than some assume. If there is a lesson to be learned from the movie, it is that the potential criminality associated with computers can be eclipsed only by the difficulty in identifying and investigating these crimes.

Discussions of emerging technological crimes center mostly on computer crime, with the inference that there is only one type of offense. This is not, however, the case, because specific categories of computer crime exist.

As computer-related crimes become more prevalent, an increasing need emerges for police personnel—particularly those who do not have expertise in computer technology—to understand how these crimes vary. An understanding of the types of computer-related crimes will assist law enforcement by providing insight for investigative strategies.

TYPES OF COMPUTER CRIMES

There are primarily four general types of computer crimes. However, in practice, multiple crimes, that is, concurrent criminality or lesser offenses, can occur during any given criminal transaction, resulting in an overlap between the classifications.

> ***"...the potential criminality associated with computers can be eclipsed only by the difficulty in identifying and investigating these crimes."***

Dr. Carter is a professor in the School of Criminal Justice, Michigan State University, East Lansing, Michigan.

Computer As the Target

Crimes in which the computer is the target include such offenses as theft of intellectual property, theft of marketing information (e.g., customer lists, pricing data, or marketing plans), or blackmail based on information gained from computerized files (e.g., medical information, personal history, or sexual preference). These crimes also could entail sabotage of intellectual property, marketing, pricing, or personnel data or sabotage of operating systems and programs with the intent to impede a business or create chaos in a business' operations.

Unlawful access to criminal justice and other government records is another crime that targets the computer directly. This crime covers changing a criminal history; modifying want and warrant information; creating a driver's license, passport, or another document for identification purposes; changing tax records; or gaining access to intelligence files.

Techno-vandalism occurs when unauthorized access to a computer results in damage to files or programs, not so much for profit but for the challenge. In such cases, the damage or loss may be intentional or accidental.

Another crime in this category is techno-trespass, that is, "walking" through a computer just to explore. In such cases, the intruder only looks at a file, but even this violates the owner's privacy. This would be the technological equivalent of a criminal trespass.

In all of these crimes, the offender uses the computer to obtain information or to damage operating programs. The offender commits the crime either by "superzapping" or by becoming a "super user." These labels mean that the offender accesses the operating program by masquerading as the system's manager, thus giving the intruder access to virtually every file in the system.

Not surprisingly, becoming a super user is relatively easy for individuals experienced in computer operations, because virtually every operating system has a trap door that allows individuals to enter a system and declare themselves the system's manager. Trap doors permit access to systems should a problem, either a human or technological one, arise. Unfortunately, this device also poses a threat to the system's integrity.

One of the best examples of a crime in which the computer is the target can be found in the book *The Cuckoo's Egg* by Cliff Stoll. The book recounts the true story of a hacker from Hanover, Germany, who infiltrated a number of computers in the United States, including those of universities, the military, and government contractors. The hacker attempted to locate and steal national security information in order to sell it to foreign governments, a clear illustration of making computers the targets of crime.

Computer As the Instrumentality of the Crime

In common law, instrumentality refers to the diversion of a lawfully possessed item, that is, an instrument, to facilitate committing a crime. In this category, the processes of the computer, not the contents of computer files, facilitate the crime.

Essentially, the criminal introduces a new code (programming instructions) to manipulate the computer's analytical processes, thereby facilitating the crime. Another method involves converting legitimate computer processes for illegitimate purposes. Crimes in this category include fraudulent use of automated teller machine (ATM) cards and accounts; theft of money

from accrual, conversion, or transfer accounts; credit card fraud; fraud from computer transactions (stock transfers, sales, or billings); and telecommunications fraud.

One example of using a computer as the instrument to commit a crime is the growing problem of individuals' using cellular phones and electronically billing charges to other customers. In these cases, offenders obtain cellular billing identification codes by using scanning devices, which are small parabolic (curve-shaped) antennae connected to portable computers. When activated, these scanners capture and store account numbers transmitted by cellular phones.

The offenders operate near highways, because motorists frequently make calls from their cars. Once they capture the computerized billing codes, they program these codes into other cellular phones simply by hooking up the phone to a personal computer. Then, using software originally developed by programmers in London, they reprogram the signal chip in the cellular phone. The use of this software, which is easy to copy and to use, is spreading across the United States and Canada, sometimes being shared through underground computer bulletin board services (BBS).

Computer Is Incidental to Other Crimes

In this category of computer crime, the computer is not essential for the crime to occur, but it is related to the criminal act. This means that the crime could occur without the technology; however, computerization helps the crime to occur faster, permits processing of greater amounts of information, and makes the crime more difficult to identify and trace. Such crimes include money laundering and unlawful banking transactions, BBSs supporting unlawful activity, organized crime records or books, and bookmaking. In one case, a suspect committed murder by changing a patient's medication information and dosage in a hospital computer.

Cases involving drug raids, money laundering seizures, and other arrests also have produced computers and electronic storage media containing incriminating information. Many times, the criminals encrypt the data or design the files to erase themselves if not properly accessed. In some instances, criminals even destroy the storage media, such as disks, to eliminate evidence of their illegal activities.

> ***"...the elements of a computer-related offense must be established for successful prosecution...."***

All of these situations require unique data recovery techniques in order to gain access to the evidence. And, in every case, the crimes could occur without the computers; the systems merely facilitate the offenses.

Another illustration of how criminals use technology to further their illegal activities involves child pornography. Historically, consumers of child pornography have trafficked photographs and related information through newsletters and tightly controlled exchange networks. Now, with the advancement of computer technology, child pornographers exchange this information through BBSs.

Recently, U.S. Customs agents raided 40 locations in 15 States serviced by a Denmark-based, child pornography BBS. These criminals used the computer to facilitate the distribution of pornographic material and to increase the efficiency of criminal activity already occurring via other methods.

Crimes Associated With the Prevalence of Computers

The simple presence of computers, and notably the widespread growth of microcomputers, generates new versions of fairly traditional crimes. In these cases, technological growth essentially creates new crime targets. Software piracy/counterfeiting, copyright violation of computer programs, counterfeit equipment, black market computer equipment and programs, and theft of technological equipment fall into this category of computer crime.

One offense in this category occurs with relative frequency—the violation of copyright restrictions of commercial software. Initially, this offense may not seem like a serious crime; yet, the potential loss to businesses can be quite staggering.

A software package usually costs about $400; a strong-arm robbery usually yields about $50 or less for the thief. Thus, *one* copyright violation is the economic equivalent of *eight* strong-arm

robberies. However, because the emotional trauma experienced in a piracy is almost nonexistent, many people do not view this as a serious crime.

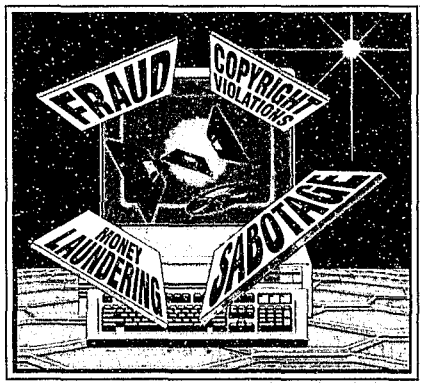
Evidence exists that software also is being written and sold explicitly to help hackers break into computers. In another area, successful computer programs—notably word processing, spreadsheets, and databases—are being duplicated, packaged, and sold illegally on a large scale, just as audio and video tapes are pirated. Similarly, counterfeit computers and peripherals (items such as modems and hard disks) are being manufactured and sold as originals in much the same manner as imitation Rolex watches and Gucci shoes.

PERSPECTIVE ON LEGAL ISSUES

Offenses vary by both the criminal act and the jurisdiction. Some States have enacted laws specifically directed toward crimes involving computers, while other States rely fundamentally on the common law as it applies to current and emerging technology. As with any other crime, the elements of a computer-related offense must be established for successful prosecution, not a particularly easy task in light of the nature of computer technology.

For example, the criminal intent, *mens rea*, of a specific computer crime may be difficult to prove. How does an investigator distinguish between a hacker who intentionally steals or destroys electronic files and someone who accidentally destroys files while simply perusing them? This is definitely not a simple question to answer, and it will continue to perplex investigators, given the nature of changing technologies and the inventiveness of the generally intelligent people who tend to commit computer-related crimes.

Similarly, the physical act of a computer-related crime, *actus reus*, may be demonstrated best by an electronic impulse that, unfortunately, is difficult to define and track, considering that a computer crime can occur in 3 milliseconds using a program code that tells the software to erase itself after the computer executes the action. Essentially, this eliminates the evidentiary trail.



These issues provide similar problems for the criminal element of causation, typically found in statutes relying on the common law. Causation in this regard relates to the self-destruction of computer programs that facilitate "cyber" crimes. How can an investigator show causation if the offender erases the executing instructions?

Additionally, the electronic data interchange (EDI) and its networks complicate the legal elements by making it more difficult for law enforcement to specify, document, and materially link the crime to an individual. The EDI connects parties via computer for contract negotiations, sales, collections, and other business transactions. The computer becomes the vault, with the EDI serving as the key to its contents. The ability to access data in the computer must be relatively easy in order to maximize business efficiency; yet, security controls must be introduced in order to protect the business' "crown jewels."

Unfortunately, maximum security and easy accessibility are not compatible. Consequently, because businesses generally prefer user-friendly equipment, system security usually takes second priority. The phenomenal growth of computer BBSs, on-line services, and the Internet only serves to compound the problem. As a result, computer-related crimes become easier to perpetrate and more difficult to identify, investigate, and prove.

SPECIAL PROBLEMS WITH COMPUTER-RELATED CRIME

Intellectual Property

Discussions of computer-related crime refer with increasing frequency to intellectual property. While the term is familiar to many, its actual meaning may be somewhat elusive.

Intellectual property consists of concepts, ideas, planning documents, designs, formulas, and other information-based materials intended for products or services that have some commercial value or represent original thoughts or theses. Crimes associated with intellectual property focus primarily on theft

when the product has commercial value, as opposed to basic research or research for private use.

In some instances, the theft takes place when a competitor manufactures a similar product developed from stolen intellectual property. In other cases, the crime occurs when the offender mounts countermarketing strategies after learning of a competitor's product through illegal, electronic means, oftentimes referred to as competitive intelligence.

Frequently, these crimes are difficult to discover and even more difficult to prove. The problem becomes further complicated when the property is still in the developmental stages with its final design or application still incomplete.

The investigation and prosecution of thefts of intellectual property with clear protection—such as intellectual property that is copyrighted or has a trademark, patent, or registered trade secret—have more of an advantage than when the protection of such property can be debated. This latter category includes unprotected research and development, original concepts and ideas yet to be realized, and public domain information modified with individual refinements. These areas provide particular challenges for investigating and proving a wrongdoing.

Intellectual property can be divided into two broad categories. The first involves formulas, processes, components, structure, characteristics, and applications of new technologies and covers such areas as fiber optics, computer chip designs and conductivity, and telecommunications equipment, protocols, and technologies, to name a few.

The second category of intellectual property takes in factors associated with the marketing and production of new technologies. Pricing information, marketing targets, product release dates, and production timetables would be included in this category.

> ***"Protocols must be developed for law enforcement that address the various categories of computer crime."***

Malfeasance by Computer

The concept of malfeasance by computer means that computer-related behavior stretches the bounds of legality and may be viewed as only technically wrong, despite its widespread, potentially negative impact. Without question, a variety of computer-related behaviors border on illegality but are not clearly defined as such. Although sometimes done with the best intent, the behavior poses ethical problems, at the very least. The following scenarios illustrate the problem:

- A parent offers to copy a computer program for a school that cannot afford to buy the software
- An employee secretly maintains a small database in an office computer as part of a sideline business
- An individual uses someone else's computer account number and password to view the contents of a database
- A customer gives her unlisted telephone number as part of a sales transaction at a store. The store enters the number into a computerized database and later sells the data to a telemarketing firm without the customer's permission
- A university computer programmer develops a program to schedule classes as part of a job assignment. The programmer then accepts a job with another university and leaves with a copy of the program for use at the new place of employment.

These illustrations point to the "gray" areas of computer abuse—areas that fall increasingly on the shoulders of law enforcement to address and resolve.

International Issues

Americans tend to have a provincial view that the United States is ahead of the rest of the world in many areas, especially technological development. While this is true to some extent, the lead is not as great as many would believe. Japan and Germany, in particular, have shown themselves to be strong technological innovators and consumers. In general, technological knowledge and expertise contribute to the growth of computer-related crime on an international level.

Americans must be concerned about the growth of computer-related crime capabilities emerging outside U.S. borders because of the ease of information exchange and the high concentration of

computer-driven businesses and research projects in the United States. However, it appears that the area of most rapid growth will be in Europe as a result of the treaties signed to create the European Community. Among the important elements of the act that established the basis for unification are open communications, a single, European-wide communication protocol, a strong profit-oriented market spanning 12 countries, open borders, unification of technology standards, and easier banking, including monetary transfers between countries.

While businesses can make great use of these unifying measures, so can criminals. Emerging international crime-related issues most probably will accompany the unification of Europe. These issues include industrial espionage (competitive intelligence), economic/political espionage, expansion of international organized crime beyond traditional areas, and theft of technological hardware.

CONCLUSION

Criminals have adapted the advancements of computer technology to further their own illegal activities. Unfortunately, their actions have far out-paced the ability of police to respond effectively.

Protocols must be developed for law enforcement that address the various categories of computer crime. Investigators must know the materials to search and seize, the electronic evidence to recover, and the chain of custody to maintain. Without question, law enforcement must be better prepared to deal with the many aspects of computer-related crimes and the techno-criminals who commit them. ✦

Bulletin Reports

NCJRS On-line

The National Criminal Justice Reference Service (NCJRS) offers access to criminal justice information through the Internet. The NCJRS gopher menus can connect users to resources of the National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention, Office for Victims of Crime, Bureau of Justice Statistics, Bureau of Justice Assistance, and Office of National Drug Control Policy. They also provide direct links to NCJRS*BBS and other criminal justice resources around the world. The gopher address is *ncjrs.aspensys.com71*

Another service offered is NCJRS World Wide Web (WWW), which provides a graphical interface to NCJRS information, as well as to information from other criminal justice resources around the world. The address for the NCJRS WWW is *http://ncjrs.aspensys.com:81/ncjrshome.html*

The Justice Information (JUST INFO) Electronic Newsletter is a free newsletter distributed on the 1st and 15th of every month. To subscribe:

1. **Type** an e-mail to *listproc@aspensys.com*
2. **Leave** the subject line blank
3. **Type** *subscribe justinfo* in the body of the message and then your name (e.g., *subscribe justinfo john doe*)

E-mail also can be used to obtain information and help from NCJRS. First-time users who send an e-mail message to *look@ncjrs.aspensys.com* will receive a reply outlining NCJRS services. For technical assistance or for answers to specific questions on criminal and juvenile justice topics, e-mail should be sent to *askncjrs@aspensys.com*