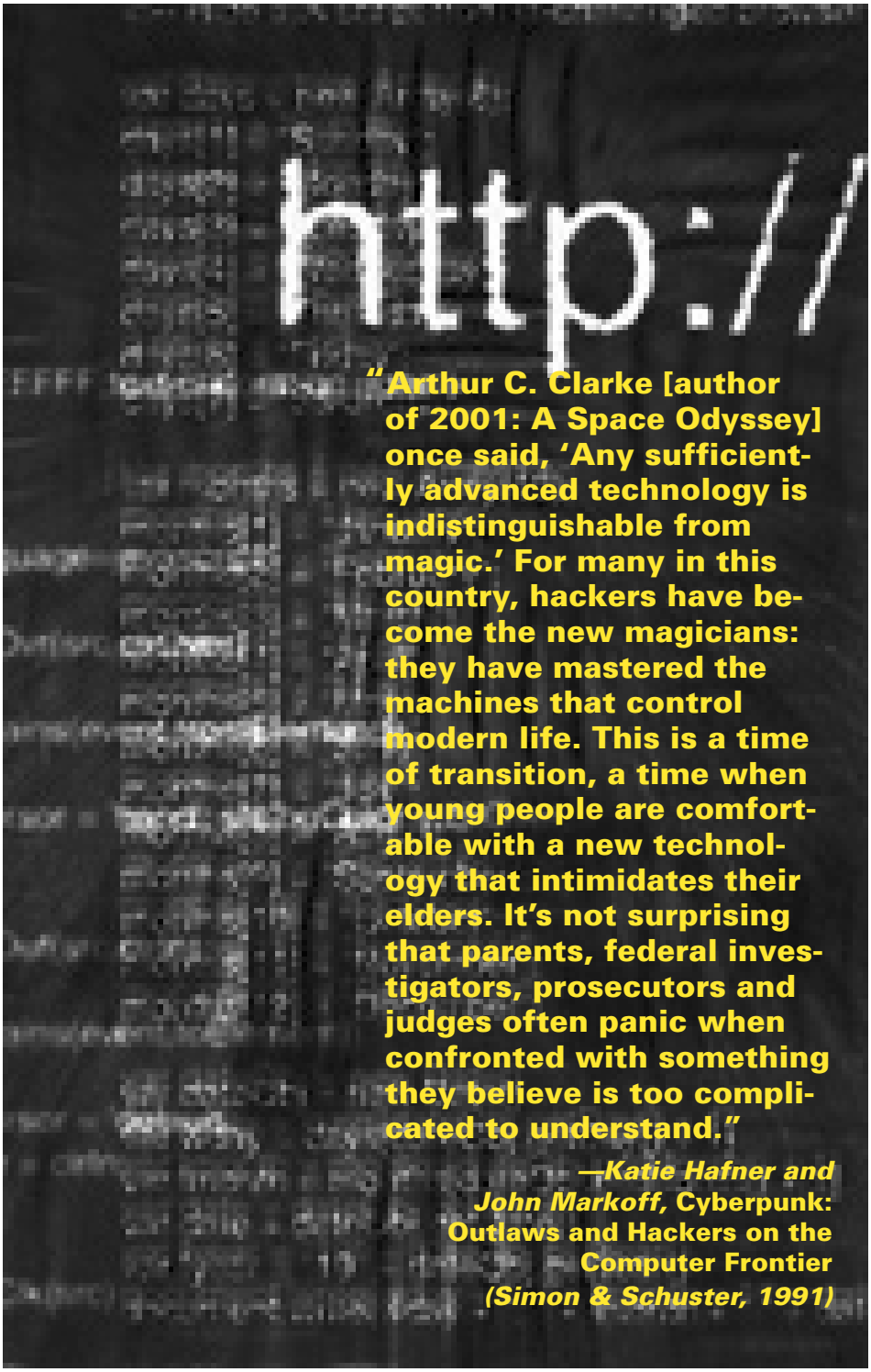
Special Needs Offenders BULLETIN

a publication of the Federal Judicial Center

No. 5
August
2000



Photodisc

"Arthur C. Clarke [author of 2001: A Space Odyssey] once said, 'Any sufficiently advanced technology is indistinguishable from magic.' For many in this country, hackers have become the new magicians: they have mastered the machines that control modern life. This is a time of transition, a time when young people are comfortable with a new technology that intimidates their elders. It's not surprising that parents, federal investigators, prosecutors and judges often panic when confronted with something they believe is too complicated to understand."

—Katie Hafner and John Markoff,* Cyberpunk: Outlaws and Hackers on the Computer Frontier *(Simon & Schuster, 1991)

Introduction to

Cyber Crime

By Mark Sherman

Cyber crime poses a daunting challenge to the federal judiciary. Consider the following:

- In February 2000 several major Internet sites—Amazon, CNN, eBay, E*Trade, and Yahoo!, to name a few—were effectively shut down by

INSIDE

an unknown assailant or group of assailants who had unleashed a wave of cyber attacks known as "distributed denial of service." These anonymous attacks are initiated when a computer hacker breaks into scores of host computers which serve a network of smaller computers. The hacker stores a slave software program on the host computers and then instructs the slave to send a message to the networked computers. The message tells the networked computers to send repeated messages to the targeted Internet sites, thus flooding them with the bogus messages and preventing legitimate users from accessing the sites.

- In December 1999 a New Jersey-based computer programmer pleaded guilty to creating the Melissa virus that infected more than 100,000 computers worldwide and caused an estimated $80 million in damages. He faces up to 57 months in federal prison.
- In April 1999 visitors to an on-line financial news message board operated by Yahoo! were greeted by a message stating that ParGain, a California-based telecommunications company, was being purchased by an Israeli company. The message referred readers to what appeared to be a web site sponsored by Bloomberg News Service containing a detailed story on the takeover. As the news spread, ParGain's publicly traded stock rose almost 30%. Unfortunately, the story was false; the "Bloomberg" site, counterfeit. As a result, ParGain's stock price nose-dived, causing significant losses to investors who had purchased the stock at inflated prices. Within a week the FBI arrested a Raleigh, North Carolina, man who had been traced through an Internet Protocol address he'd used. He was charged with securities fraud and sentenced to five years of probation with five months home of detention and was ordered to pay $93,000 in restitution.
- A recent federal case in the Southern District of Florida involved a college-educated defendant with no criminal history. The defendant, located in Arizona, downloaded files from a child pornography chat room on the Internet and transmitted them electronically to an undercover police officer in Miami. He was charged with violating federal child pornography laws and released on bond. Release conditions specified no computer access as well as no contact with children. Electronic monitoring was also ordered. During his release, the defendant lived in Arizona with his mother, who was a computer teacher. She was prohibited from using a computer in her home. Beyond that, the issue of how to monitor the defendant's compliance with the computer-specific condition was unresolved. Defense counsel had the defendant undergo a mental health evaluation which determined that he was a potential pedophile. The case ended in a plea agreement resulting in a prison term of 24 months.

These are but a few examples of the "cyber criminals" increasingly occupying the federal criminal justice system. According to the Electronic Privacy Information Center, a research and advocacy organization based in Washington, D.C., the number of computer crime cases referred to federal prosecutors jumped by 43% in 1998 over the previous year.

Recently, the Northern District of Ohio probation office began keeping statistics on computer offenders in the district. Using PACTS data, the district identified 28 such offenders over a year. The offenders ranged from minimally skilled bank tellers and government employees who unlawfully accessed their employers' computer systems to computer-savvy child pornographers and hackers.

In light of these trends, officers must further their knowledge of how computers, "connected devices" (e.g., wireless phones and handheld computers), and networks function and how they are used to commit crimes. Further, they must be able to combine conventional and cyber-specific investigation and supervision techniques to help courts fashion appropriate sentences and release conditions and to monitor compliance. This *Special Needs Offenders Bulletin* introduces officers to cyber crime by providing case examples, defining terms, suggesting investigative questions and release conditions, and addressing technical and legal issues that officers must bear in mind. ◆

STORY OF A "CYBERPUNK"

Cyber crime presents two basic challenges for probation and pretrial services officers. First, defendants and offenders involved in cyber crime can possess skills far beyond those of even the most technologically "smart" officer. Second, supervising these individuals may pose problems not unlike those associated with sex offenders and others driven by psychological compulsions.

One of the world's most well-known cyber criminals is Kevin Mitnick. Mitnick is a computer hacker who recently embarked on a three-year term of supervised release in the Central District of California. Although extreme, Mitnick's case illustrates the types of crime that federal probation and pretrial services officers are now up against.

Mitnick grew up in middle-class circumstances in southern California in the 1970s and '80s. His parents divorced when he was three, and his mother, with whom he lived and who worked full time, subsequently married and divorced several more times. As a teenager, Mitnick became bored with school but obsessed with telephones and two-way radios. He and several like-minded friends taught themselves about telephone and radio hardware and figured out ways to steal information and long-distance service from telephone companies. Their methods included searching the trash bins of Pacific Bell (known as "trashing" or "dumpster diving") and impersonating telephone company employees to get account information from customers. Mitnick and his pals had become "phone phreaks." Soon they began sharing methods and information through a computer bulletin board—posting and acquiring stolen credit card and calling card numbers, computer passwords, and technical information on phone networks.

Gradually, Mitnick progressed from phone phreaking to unlawfully accessing business and government computers. Using stolen MCI long-distance codes and a Radio Shack personal computer connected to a modem, Mitnick would log on to commercial computers via the Telnet, a telephone system through which computers "speak" to each other by sending small packets of data back and forth. He became adept at breaking into Pacific Bell's computer systems and redirecting and altering customers' phone bills. Working with colleagues, he broke into U.S. Leasing's mainframe computer and jammed its business operating systems. He also accessed the computer systems of the University of Southern California, the Defense Department, defense contractors, and others. (Both the USC and U.S. Leasing mainframes, designed by Digital Equipment Corp., were notoriously insecure.)

Eventually, Mitnick was arrested for the U.S. Leasing and USC break-ins. For the former, he received a one-year juvenile probation sentence. For the latter, he served just over eight months in a juvenile detention facility.

In the years after his release, Mitnick resumed hacking, breaking into Santa Cruz Operations, a computer consulting firm. He was arrested and pleaded *nolo contendere*. The municipal court sentenced Mitnick to probation and imposed a fine. His subsequent break-in at Digital in 1988 attracted the attention of the FBI. Ultimately, Mitnick was apprehended and brought before a U.S. magistrate judge who ordered him detained pending trial. He cooperated with federal prosecutors against a fellow hacker and received a one-year prison sentence followed by a six-month treatment program. His lawyer had convinced the court that Mitnick was a computer "addict," suffering from a compulsion. The terms of his supervised release initially prohibited him from using a computer, but the conditions were altered so that he could seek computer-related employment.

In 1992, Mitnick once again became the target of an FBI investigation after he was discovered illegally using a commercial database. A federal

Computer Bulletin Boards

A bulletin board system (BBS) is a space on a computer created by a user for discussion with others on a specific topic. Some BBSs allow users to legally upload, store, and download software known as "shareware." As the number of BBSs grew throughout the 1980s, so did the number of systems providing pirated software and explaining how to override software features that prevent copying.

Read more about Kevin Mitnick!

Two best-selling books have been written about Mitnick, hackers, and the challenges posed by cyber crime: *Cyberpunk*, by Katie Hafner and John Markoff (Simon & Schuster, 1991) and *Takedown*, by Tsutomu Shimomura and John Markoff (Hyperion, 1996).

judge issued a warrant for his arrest for violating his release conditions. Eluding authorities, Mitnick hacked into the systems of cellular telephone manufacturers, Internet service providers, and universities, from which he stole and stored copies of the software that control cellular telephones.

Finally, in 1995, the FBI apprehended Mitnick in Raleigh, North Carolina. He pleaded guilty to one count of cellular telephone fraud and was sentenced to eight months in prison. However, following completion of that sentence, he remained in jail pending new charges, including release violations. Ultimately, he was indicted on 25 counts accusing him of causing $80 million in damage by breaking into corporate computers (those of Motorola, Sun Microsystems, NEC, and Novell, to name only a few) and stealing software, product plans, and other data. Plea negotiations continued through March 1999, when an agreement was struck in which Mitnick conceded that he caused $5 million to $10 million in damage.

Ultimately, Mitnick was sentenced to another ten months in prison and ordered to pay $4,125 in restitution. He was released from prison in January 2000. He will be on supervised release for the next three years subject to several cyber-specific conditions: He is not permitted access to any connected device save a landline telephone. Specifically, he is prohibited from possessing or using computer hardware, software, modems, computer-related equipment, laptop computers, personal information assistants, cellular telephones, computer-accessible televisions, or other communications instruments that can be connected to the Internet or telecommunications networks. He is also barred from working in a computer, software, or telecommunications business or in any job where he has access to computers, computer-related equipment, or software.

Cases like Mitnick's present particular challenges for pretrial services and probation officers. With regard to investigation, pretrial services officers and presentence report writers, in order to tailor and recommend special release conditions, must evaluate a defendant's or offender's access to and ability with computers and understand how cyber crimes are committed (see boxes on pp. 11 and 12). With regard to supervision, pretrial services and probation officers must consider, among other things, how to monitor compliance with cyber-specific special conditions.

A Cyber Crime Supervision Success Story: Kevin Poulsen: Ex-cyberpunk

A notable cyber crime success story for federal probation is that of hacker Kevin Poulsen. Poulsen was arrested in California by the FBI and convicted of money laundering and wire fraud. His crimes included using computers to rig radio phone-in contests (his winnings included a trip to Hawaii and a Porsche). He was held without bond for 51 months, and his sentence included a three-year term of supervised release. Poulsen's release conditions prohibited him from using computers and the Internet. Initially, his relationship with his probation officer was adversarial. By November 1998, however, the tenor of the relationship had changed for the better, and, upon a recommendation from his probation officer, the U.S. District Court for the Central District of California modified Poulsen's release conditions to allow Internet access. Poulsen completed his term of supervised release in June 1999 and has gone on to become a reporter for ZDTV and SecurityFocus.com.

WHAT IS CYBER CRIME?

Cyber crime is difficult to define because it ranges from crimes that cannot be committed without a computer or connected device to traditional crimes that are merely facilitated by computers or connected devices. In its March 2000 report, the President's Working Group on Unlawful Conduct on the Internet provided a helpful framework for thinking about cyber crime. According to the Working Group, cyber crime can be carried out in one of three ways:

- *Computer as object, victim, or target*. Crimes in this category involve attacks on the confidentiality, integrity, or availability of a computer's information or services, i.e., targeting a computer system to acquire stored information, steal services, corrupt data, or interfere with the accessibility of the computer or server.
- *Computer as subject or storage device*. Unlawful conduct of this type involves using a computer or connected device to store data used in carrying out criminal activity, e.g., transmitting a computer program containing instructions to trigger a malicious act automatically.
- *Computer as instrument or tool*. With this type of criminal conduct, a computer, network, or connected device is used to make traditional unlawful activity easier and faster.

The most common types of cyber crime confronted by pretrial services and probation officers include child sexual exploitation, securities and credit card fraud, network manipulation, and hacking or cracking.

Child sexual exploitation can be committed with computers in different ways, for instance, when users knowingly send or receive pornographic images of children in files attached to e-mails or when they access Internet chat rooms or computer bulletin boards and knowingly download images posted by others. A related activity is using chat rooms or bulletin boards to lure minors into sexual liaisons. The U.S. Sentencing Commission has recently amended the U.S. Sentencing Guidelines (USSG) to account for these types of crimes.

Fraud perpetrated with computers—particularly credit card fraud—is becoming increasingly prevalent. Offenders use either Credit Master or Credit Wizard software to generate accounts. The software is free and can be downloaded from web sites that make it available. Federal legislation currently pending would criminalize use of software to create fraudulent credit card accounts.

Network manipulation is typically committed by a disgruntled or former employee who accesses a company's computer system to steal money or to obtain proprietary information for sale to a third party or for extortion purposes.

Hacking/cracking involves breaking into a computer system, often by obtaining passwords or confidential access information through deceit (re

Cyber Crime Types

Computer as object, victim, or target
(Offender targets computer itself.)

- theft of computer processor time and computerized services
- denial of service
- other hacking/cracking crimes where the computer is the target

Computer as subject or storage device
(Computer is physical site of crime or source of or reason for unique forms of asset loss.)

- viruses
- Trojan horses
- logic bombs
- sniffers
- cell phone cloning

Computer as instrument or tool
(Computer is used to commit traditional crimes.)

- credit card fraud
- money laundering
- counterfeiting
- child sexual exploitation (e.g., child pornography, child luring)
- gaming
- identity theft
- intellectual property theft

Characteristics of Defendants and Offenders Involved in Cyber Crimes

According to a 1996 U.S. Sentencing Commission report, defendants in white collar (including fraud, forgery/counterfeiting, and money laundering) and computer fraud cases typically have no criminal history and are:

- U.S. citizens
- male
- white
- college graduates or high school graduates with some college

For more information on cyberstalking

See "Cyberstalking: A New Challenge for Law Enforcement and Industry: A Report from the Attorney General to the Vice President" (August 1999). *http://www.usdoj.gov/ag/cyberstalkingreport.htm*

ferred to as "social engineering") to steal information, corrupt data, or jam transmissions. A closely related crime is cell phone cloning in which the account number of a victim's cellular telephone is stolen and reprogrammed into another cellular phone. The 1998 Wireless Telephone Protection Act amended the federal statute governing fraud and related activity in connection with access devices. The U.S. Sentencing Commission has recently amended the USSG to accommodate this new law.

Several other cyber crimes have already found or soon may find their way onto federal criminal dockets and will pose challenges for officers in the near future. These crimes include identity theft, software and recording piracy, cyberstalking, and counterfeiting.

Identity theft involves appropriation of a person's identifying information for unlawful purposes. Computers often figure in this activity. In 1998 the Identity Theft and Assumption Deterrence Act (18 U.S.C. § 1028(a)(7)) became law, and the Sentencing Commission has recently amended the USSG to accommodate it.

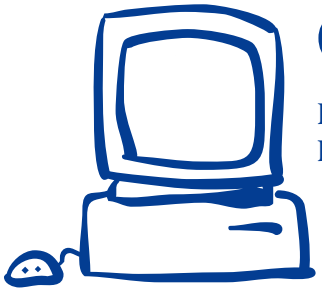
Software and recording piracy involves infringing on the copyright and trademark protection afforded to intellectual property, including software for programming computers and connected devices, and audio and video recordings. Because many recordings have been digitized, they can be uploaded via computer onto the Internet and then downloaded for playing, copying, or bootlegging.

The Software and Information Industry Association notes that software piracy accounts for an estimated $11 billion loss in annual software revenues worldwide. Recent legislation to address these issues includes the No Electronic Theft (NET) Act of 1998 and the Digital Millennium Copyright Act (DMCA) of 1998. The Sentencing Commission has recently amended the USSG to accommodate these new laws.

"Cyberstalking" is defined as using the Internet, e-mail and other electronic communications to harass or threaten. In a recent case prosecuted under California's cyberstalking law, a 50-year-old man pleaded guilty to stalking and other charges for soliciting the rape of a 28-year-old woman who had rejected his advances. The man impersonated the woman in Internet chat rooms, posting her telephone number and address along with messages that she had fantasies of being raped. On several occasions men knocked on the woman's door saying they wanted to rape her.

Counterfeiting. According to a recent memo to chief probation officers from AO/FCSD Director John M. Hughes, "computer technology has changed the nature of production methods used in counterfeiting. Operations have evolved from the traditional method of offset printing to using personal computers connected to scanners or digital input devices, together with inkjet printers, and full color copiers." Images can be uploaded from a personal computer to the Internet and transmitted to other users who have no specialized knowledge of computers or graphics. Hughes observed that the Secret Service is concerned that USSG 2B5.1(b) might not reflect the change in the nature and harm caused by such high-tech methods. He noted that "the Secret Service suggests that officers in appropriate cases consider including in the offense-level section of the presentence investigation report a brief statement regarding the new technology, simply highlighting the differences between traditional and current, state-of-the-art counterfeiting techniques."* ◆

*Note: This memo can be downloaded from the J-net at http://156.119.80.10/programdesk/fcsd/html/memos/fcsd99044.htm.



COMPUTER BASICS

If you're new to computers, the Administrative Office of the U.S. Courts, Program and Workforce Development Division (PWDD) offers courses for court staff in word processing and using the Intranet/Internet. For more information, contact the PWDD at (202) 502-1660.

Following are descriptions of basic computer components:

CD-ROM (Compact Disk Read-Only Memory) a platter (CD) on which massive amounts of information can be stored. A *laser disk drive* is similar to a CD ROM drive but uses lasers to read and store information.

central processing unit (CPU) an older term for processor and microprocessor, the central unit in a computer containing the logic circuitry that performs the instructions of a computer's programs.

directory a named group of related files. A directory's name separates it from other groups of files.

fax peripheral a device, normally inserted as an internal card, that allows a computer to function as a fax machine.

file in any computer system but especially in personal computers, an entity of data available to system users (including the system itself and its application programs) that is capable of being manipulated as an entity (for example, moved from one file directory to another).

floppy disk drive a mechanism that reads data on or saves data to "floppy" diskettes. Information is stored on the diskettes themselves, not on the drive.

hard disk drive a fixed component on which software applications and data may be stored.

keyboard a primary text input device. The keyboard also contains certain standard function keys, such as the Escape key, tab and cursor movement keys, shift and control keys, and sometimes other manufacturer-customized keys. The computer keyboard uses the same key arrangement as the mechanical and electronic typewriters that preceded the computer.

modem a device allowing a computer to communicate with another computer, normally over standard telephone lines. Modems may be either external or internal.

monitor a computer screen and related parts packaged in a physical unit that is usually separate from other parts of the computer. In practice, the terms monitor, screen, and display are used interchangeably.

mouse a pointing device that controls input. Normally, the user points to an object on the screen and then presses a button on the mouse ("clicks") to indicate the selection.

operating system a program that manages all the other programs in a computer. The other programs are called *applications*.

printer a device linked to a computer to provide output on paper. Dot matrix printers produce characters and graphics with pins that strike ribbon and paper. Laser printers electrostatically charge the printed page and apply toner. Ink jet printers spray ink onto the paper. Thermal printers have a hot printer head that contacts special paper which reacts to heat. Band printers have a rotating metal band that is struck. Daisy wheel printers have a small print wheel containing each character. Plotter printers move ink pens over the paper surface; they are typically used for large engineering and architectural drawings.

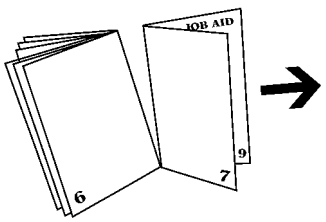
scanner any optical device that can recognize images on paper and, using specialized software, convert them into digital form.

software programs used to operate computers and related devices. Software is often divided into application software (programs that do work users are directly interested in) and system software (which includes operating systems and any program that supports application software).

Zip drive (or Jaz drive) a small, portable disk drive used primarily for backing up and archiving personal computer files.

Applicable Statutes and Guidelines for Cyber Crimes: A Job Aid for Presentence Report Writers

Type of Unlawful Conduct	Examples of Applicable Federal Laws	Examples of Applicable Sentencing Guidelines*
Computer, Internet, and Wireless Fraud	5 U.S.C. §§ 45, 52	No applicable guideline
	15 U.S.C. § 1644	§2F1.1**
	18 U.S.C. § 1028	§§2F1.1, 2L2.1, 2L2.2
	18 U.S.C. § 1029	§2F1.1
	18 U.S.C. § 1030	§§2B1.1**, 2B1.3, 2B2.2, 2B2.3, 2F1.1, 2M3.2, 2X1.1
	18 U.S.C. § 1341 et seq.	§2F1.1
	18 U.S.C. § 1345	No applicable guideline
	18 U.S.C. § 1956	§2S1.1
	18 U.S.C. §1957	§2S1.2
On-line Child Pornography, Child Luring, and Related Activities	18 U.S.C. § 2251 et seq.	§§2G1.1**, 2G2.1**, 2G2.2**, 2G2.4**
	18 U.S.C. § 2421 et seq.	§§2G1.1, 2A3.1**, 2A3.2**, 2A3.3**, 2A3.4
Internet Sale of Prescription Drugs and Controlled Substances	15 U.S.C. § 45 et seq.	No applicable guideline
	18 U.S.C. § 545	§§2Q2.1, 2T3.1
	18 U.S.C. § 1341 et seq.	§2F1.1
	21 U.S.C. § 301 et seq.	No applicable guideline
	21 U.S.C. §§ 822, 829	No applicable guideline
	21 U.S.C. § 841	§§2D1.1, 2D1.9, 2D1.11, 2D1.13, 2D2.1; §2D1.7
	21 U.S.C. § 863	No applicable guideline
	21 U.S.C. § 951	§2D1.1
	21 U.S.C. §§ 952–953	§2D3.2
	21 U.S.C. § 954	§2D1.1
	21 U.S.C. § 955	§2D1.1
	21 U.S.C. § 957	§2D1.1
	21 U.S.C. § 958	No applicable guideline
	21 U.S.C. §§ 959–961	§§2D1.1, 2D1.11, 2D1.13, 2D3.1; §2D3.2
	21 U.S.C. § 963	§§2D1.1, 2D1.2, 2D1.5–2D1.13, 2D2.1, 2D2.2, 2D3.1



This job aid can be removed for posting.

Applicable Statutes and Guidelines for Cyber Crimes: A Job Aid for Presentence Report Writers

Type of Unlawful Conduct	Examples of Applicable Federal Laws	Examples of Applicable Sentencing Guidelines*
Internet Sale of Firearms	18 U.S.C. § 921 et seq.	§§2K2.1, 2K2.4, 2K2.5, 2A1.1–1.4
Internet Gambling	5 U.S.C. § 3001 et seq. 18 U.S.C. § 1084 18 U.S.C. § 1301 et seq. 18 U.S.C. § 1952 18 U.S.C. § 1953 18 U.S.C. § 1955 28 U.S.C. §§ 3701–3704	No applicable guideline §2E3.1 §2E3.1 §§2E3.1, 2E1.3, 2E1.4 §2E3.1 §2E3.1 No applicable guideline
Internet Sale of Alcohol	18 U.S.C. 1261 et seq. 27 U.S.C. §§ 122, 204	No applicable guideline No applicable guideline
Online Securities Fraud	15 U.S.C. § 77(e), 77(q), 77(x) 15 U.S.C. §§ 77(j), 78(l), 78(o) 15 U.S.C. § 78(j) 15 U.S.C. § 78(ff)	§2F1.1 No applicable guideline §§2F1.1, 2F1.2 §§2B4.1, 2F1.1
Software Piracy, Intellectual Property Theft, and Counterfeiting	17 U.S.C. § 506 17 U.S.C. § 1201 et seq. 18 U.S.C. § 545 18 U.S.C. § 470 et seq. 18 U.S.C. §§ 1341, 1343 18 U.S.C. § 1831 et seq. 18 U.S.C. §§ 2318–2320	§2B5.3** No applicable guideline §§2Q2.1, 2T3.1 §§2B5.1, 2F1.1 §§2C1.7, 2F1.1 §2B1.1 §2B5.3

*Application of guidelines contained in chapter 3 (special skill, abuse of position of public trust, or vulnerable victim) and chapter 5 (grounds for departure) of the *Guidelines Manual* also may be appropriate.

**Effective date, as amended: November 1, 2000 (unless modified or rejected by Congress).

This job aid was prepared with the assistance of Jeanneine Gabriel, senior training and technical specialist with the U.S. Sentencing Commission's Office of Education and Sentencing Practice.

CYBER CRIME FAQs

Q: *I have to recommend a release condition to the court for a sex offender who used a computer in his crime. How should I word the condition?*

A: The court should consider prohibiting computer possession and use, unless permitted by his pretrial services or probation officer.

Q: *I am a pretrial services officer, and the court has ordered that close monitoring be made of a defendant's computer and Internet activities. What should I do first?*

A: Monitoring may mean periodically questioning the defendant as to how his computer is being used, what Internet sites he is visiting, and how he is using Internet e-mail. The next level of monitoring requires a computer search. Pretrial services officers should not conduct searches without specific direction from the court.

Q: *Is it true that probation officers can search offenders' computers as needed?*

A: Probation officers do not have search authority absent a special condition. The Criminal Law Committee's Model Search and Seizure Guidelines define the legal standard for conducting searches. Districts considering adopting cyber search policies and special conditions should comply with the Guidelines or should consider adopting the Guidelines if they have not already done so.

Q: *Does using an automatic teller machine (ATM), global positioning system (GPS), or handheld electronic device such as a Palm Pilot constitute computer use?*

A: Each of these devices is computer controlled and may be restricted under a computer prohibition special condition. The condition should permit the officer to decide what is a restricted computer and what is a computer-controlled appliance. Palm Pilots and Windows-based, handheld personal computers should be considered computers.

Q: *We have a district search-and-seizure policy and want to designate one or two probation officers to conduct cyber searches. What training is needed?*

A: It is strongly advised that officers conducting computer searches obtain formal training in basic computer forensics. Some training programs offer computer basics before moving into the forensic phase. Others expect a level of computer familiarity before admission to the program (see Resources for Technical Assistance and Training, p. 14).

Q: *Should we take our office system administrator with us in the field to inspect offenders' computers?*

A: No. Systems personnel have neither the training nor personnel classification necessary to join officers in the field.

Q: *We would like to take computers and diskettes we confiscated to our systems personnel to analyze. Is this appropriate?*

A: Do not use your systems personnel or other office staff for computer forensic duties unless they possess the specific qualifications and equipment to perform such tasks.

Q: *What is the least intrusive type of computer search?*

A: A directory search.

ISSUES AND TOOLS FOR INVESTIGATION AND SUPERVISION

Investigation

In terms of relevant investigative skills, both pretrial services officers and presentence report writers must know how cyber crimes are committed and must develop cyber-specific questions for the defendant or offender, collateral contacts, and the case agent.

Pretrial services officers must avoid questions about offense conduct. Defense counsel will typically object to any request for a mental health evaluation because of the possible divulgence of information related to the offense and to sentencing enhancement factors. Still, the pretrial services officer may want to request an evaluation if the defendant presents other indicators of adverse mental health.

Presentence report writers must recommend release conditions that are authorized by law and are reasonably enforceable. They must understand the scope and complexity of the offense conduct, the offender's sophistication, appropriate use of sentencing enhancements, and calculation of restitution.

Supervision

Traditional supervision techniques such as collateral contacts and record examination should be used. Also, officers supervising defendants and offenders involved in cyber crime may wish to observe the individuals' trash for evidence of computer printouts and visually inspect dwellings for empty phone jacks, which could indicate use of a connected device other than a landline telephone.

Fashioning special conditions. Developing and recommending special conditions of release in cyber crime cases is extremely challenging. Anecdotal evidence indicates that the best approach is to combine conventional and cyber-specific special conditions.

Officers may be concerned about third-party risk issues for a defendant or offender employed in a technical position when there is no special condition prohibiting such employment. The officer's approach to third party notification and supervision of a defendant who is a computer systems manager, for example, should be similar to that taken with a defendant who is an accountant, bookkeeper, financial officer, or bank teller charged with a financial crime.

With regard to monitoring, cyber crime presents significant difficulties, and districts are experimenting with different approaches. The probation office for the Middle District of Pennsylvania is requiring the use of

Suggested Pretrial and Presentence Investigation Questions

Employment-oriented questions for defendants and offenders in cyber crime cases might include:

- What need do you have for computers at your job?
- What do you use computers for?

Additional questions for the defendant or offender might include:

- Do you have family members or friends who live nearby and possess computers?
- Do you have access to a library? (Public and private libraries often maintain computers with Internet access for patrons.)
- Who else has access to or uses your computer(s)?

Questions for collateral contacts might include:

- How many computers do you have in your home?
- What types of computers do you have in your home?
- Do you maintain on-line service accounts?
- How do you use your computer(s)?
- Who else has access to or uses your computer(s)?

The pretrial services officer or presentence report writer must assess how the answers to these questions relate to the nature and seriousness of the (alleged) offense in order to fashion recommendations for release conditions. Pretrial services officers should also develop questions that will help determine whether the defendant will benefit from mental health treatment if indicators are present, while avoiding reference to offense-related conduct.

Matrix of Conventional and Cyber-specific Special Conditions

Preliminary questions

In fashioning and recommending special conditions from this matrix, officers should ask themselves the following questions:

- How was the (alleged) offense committed?
- What kinds of conditions are available?
- What are the conditions supposed to do?
- What conditions are useful for this kind of offense?
- Are the conditions a deterrent?
- Are the conditions "least restrictive"? (pretrial)
- Are the conditions enforceable?
- Do the conditions reduce risk of nonappearance? (pretrial)
- Do the conditions protect the public?
- Do the conditions facilitate rehabilitation? (probation)

Conventional special conditions

- must provide monthly telephone bills
- must provide lists of on-line accounts, screen names and passwords
- house arrest/electronic monitoring
- third-party warning/warning to custodian
- no access to pornography (child sexual exploitation cases)
- no unsupervised association or contact with children (child sexual exploitation cases)
- mental health or sex offender evaluation and treatment (where appropriate)
- occupational restriction
- search condition

Cyber-specific special conditions

- no access to the Internet or to bulletin board systems
- no access to a modem
- no access to a computer or a connected device (except a landline telephone) at any time
- no use of encryption
- no use of a detection software inhibitor
- use of filtering/screen-recording software
- consent for officer to access Internet service provider account records

filtering software—a commercial application known as Net Nanny—on the computers of offenders convicted of child sexual exploitation. The software restricts access to pornographic Internet sites. While Net Nanny can be circumvented easily by a skilled computer user, it offers some assistance with monitoring.

The probation office for the Middle District of Florida is developing an on-line check-in for offenders with Internet access. Offenders will be required to check in with the district electronically—and thus permit monitoring—whenever they access the Internet.

The Southern District of New York probation office uses commercial screen-recording software to monitor cyber offenders. The software records all activity, as a videocassette recorder does, and allows the officer to play back the recorded information. It automatically records all applications, including financial programs, databases, web sites, e-mail, and on-line chat by taking screen shots. The software can be configured to take the shots as often as the officer deems necessary. Moreover, it is password protected and more secure than filtering software.

Search and seizure. The search and seizure of computer hardware, software, or connected devices is legally and technically complex. The nature of a cyber search or seizure requires specific forensic investigative knowledge and skill, which should be acquired through training (see Resources

Alternatives to Search or Seizure

The Criminal Law Committee has recommended that, where possible, officers avoid using searches and seizures as a means of supervision. Alternatives to searches and seizures include:

- relying on the deterrent effect of conditions
- interviewing the offender
- interviewing collateral contacts
- plain view observation
- contact with other law enforcement agencies, including referral for investigation
- modifying conditions based on existing information

for Technical Assistance and Training, p. 14). A mishandled search or seizure can cause significant problems for officers and agencies. For example, probation and pretrial services officers and agencies risk exposure to civil liability if a search or seizure of networked devices is alleged to have contributed to a company's financial loss. Further, failure to follow strict legal and technical guidelines in searching or seizing computer hardware, software, or connected devices can harm or cause the loss of evidence that could be used in future prosecutions of a defendant or offender. Ultimately, while anecdotal evidence from the field suggests that search conditions have a deterrent value, searches pursuant to such conditions also carry significant risks.

What is a "search"? Monitoring the use of a specific computer or connected device through examination of its hardware or software constitutes a search. Searches or seizures of any kind by pretrial services officers are not specifically authorized by statute and are not included in the model search and seizure policy promulgated by the Criminal Law Committee; they should not be performed unless ordered by the court. In pretrial situations, the best special condition might be "no access to a computer or connected device at any time." But whether this fits the "least restrictive" requirement depends on the alleged offense. Searches or seizures of any kind by probation officers should be conducted pursuant to a specific district policy that provides clear guidelines, such as the model search policy.

The legal standard for a probation search or seizure under the model search policy is whether the officer has "reasonable suspicion" that a search will detect contraband or evidence of criminal activity. Importantly, this standard is less stringent than the "probable cause" standard for law enforcement. Therefore, probation officers may have greater discretion than law enforcement officers, which can lead to abuse or the use of probation as stalking-horse for law enforcement. Also, because the Federal Rules of Evidence are not applicable in revocation proceedings, probation officers have greater latitude than law enforcement officers in conducting searches. However, again, it also provides greater opportunity for abuse, as well as for corruption of evidence that could be used in a prosecution. ◆

Examples of Cyber Crime Case Law Involving USSG Application

- **Hacking**. *U.S. v. Petersen*, 98 F. 3d 502 (9th Cir. 1998), involved an enhancement for special skill pursuant to USSG §3B1.3.
- **Network manipulation**. *U.S. v. Williams*, 966 F. 2d 555 (10th Cir. 1992), an embezzlement case, involved an enhancement for more than minimal planning under USSG §2B1.1.
- **Child pornography**. *U.S. v. Hibbler*, 159 F.3d 233 (6th Cir. 1998), involved a five-level increase for distribution of child pornography via the Internet despite no "pecuniary gain" under USSG §2G2.2.

Other possible adjustments might relate to the use of a juvenile hacker by an adult (§3B1.4) and the obstruction of justice enhancements for destruction of evidence by computer (§3C1.1).

RESOURCES FOR TECHNICAL ASSISTANCE AND TRAINING

Technical assistance

Use of systems personnel. Systems personnel should not be taken into the field to perform searches because they possess neither the appropriate training nor the appropriate personnel classification. Nor, as a general rule, should they search computers or storage devices (hard disks, zip disks, diskettes, magnetic tape, etc.) brought by officers from the field to the office. Computer forensics requires specific tools and methods to prevent data corruption. Only persons trained in computer forensics should conduct searches. However, in developing cyber-specific special release conditions, districts may find it helpful to consult systems personnel, who can provide general information on computers, storage and connected devices, and networks.

Use of law enforcement personnel. The U.S. Secret Service Financial Crimes Division, Electronic Crimes Branch, provides technical assistance clearinghouse services. The branch can be reached at (202) 406-5850.

Training resources

The following resources are available to districts contemplating further training in computer forensics.

- The International Association of Computer Investigative Specialists (IACIS) offers a two-week Certified Computer Forensics Examiner course. Conducted twice a year, the course starts with computer basics. Cost for the Spring 2001 session is $1,195. (IACIS says the course fills up quickly). *www.cops.org*
- The National White Collar Crime Center (NW3C) offers a one-week Basic Data Recovery and Analysis course. Delivered nationwide, the popular course assumes familiarity with DOS, Windows, and computer hardware. The course is funded by the Department of Justice and is free. *www.cybercrime.org*
- The National Consortium for Justice Information and Statistics offers "The Seizure and Examination of Microcomputers" course. Conducted in Sacramento, California, the three-day entry-level course costs $242. Enrollment is limited. *www.search.org*
- Guidance Software, Inc., offers a four-day "Computer Forensic Training" course that the company says will bring participants "up to speed in the fast-paced area of computer forensics." Cost is $1,500 (discounted for those who have purchased the company's EnCase computer forensic software tool). *www.guidancesoftware.com*
- The National Center for Missing & Exploited Children offers "Protecting Children On-line," a four-day workshop providing basic instruction in computer investigation of child exploitation crimes. This is not a forensics course. The free workshop is funded by the Department of Justice. Times and locations vary. *www.foxvalley.tec.wi.us/ojjdp/*

Special Needs Offenders Bulletin

a publication of the Federal Judicial Center

No. 5, August 2000

Written by
Mark Sherman
Education Specialist
Court Education Division

Edited and designed by
Nathan Dotson
Communications Policy & Design

Send questions or comments to Mark Sherman, Court Education Division, Federal Judicial Center, Thurgood Marshall Federal Judiciary Building, One Columbus Circle, N.E., Washington, D.C. 20002-8003.

This publication was undertaken in furtherance of the Center's statutory mission to develop and conduct education programs for judicial branch employees. The views expressed are those of the author and are not necessarily those of the Federal Judicial Center.

CYBER TERMINOLOGY

General terms

bulletin board system (BBS) a computer that can be reached by computer modem dialing (and, in some cases, by Telnet) for the purpose of sharing or exchanging messages or other files. Some BBSs are devoted to specific interests; others offer a more general service. The definitive BBS List says that there are 40,000 BBSs worldwide.

data the information stored in a computer.

hardware the physical components or equipment that make up a computer system. Examples include keyboards, monitors, and printers.

host any computer that has full two-way access to other computers on the Internet. A host has a specific "local or host number" that, together with the network number, forms its unique Internet Protocol (IP) address. If you use PPP to get access to your access provider, you have a unique IP address for the duration of any connection you make to the Internet, and your computer is a host for that period. In this context, a "host" is a node in a network. The term generally means a device or program that provides services to some smaller or less capable device or program.

HTML (Hypertext Mark-up Language) the set of symbols or codes inserted in a file intended for display on a World Wide Web browser such as Netscape or Microsoft Internet Explorer. HTML tells the Web browser how to display Web page words and images for the user. The individual mark-up codes are referred to as elements (or tags).

Internet the worldwide "network of computer networks" providing file transfer, remote log-in, electronic mail, news, and other services.

Internet Protocol (IP) the most important of the protocols on which the Internet is based. IP allows a packet of data to traverse multiple networks on the way to its final destination.

network a system of interconnected computer systems and terminals.

software the programs or instructions that tell a computer what to do, including system programs that control the internal operation of the computer system (such as the Microsoft Disk Operating System—MS-DOS—which controls IBM-compatible personal computers) and application programs that enable the computer to produce useful work (e.g., word-processing programs such as WordPerfect).

system administrator (or system operator ("sysop"), or system manager) the individual responsible for ensuring that a computer system is functioning properly. He or she is often responsible for computer security as well.

server in general, a computer program that provides services to other computer programs in the same or other computers. The computer in which a server program runs is also frequently referred to as a "server," though it may contain a number of server and client programs. Specific to the World Wide Web, a Web server is the computer program (housed in a computer) that serves requested HTML pages or files. The Web browser in a computer requests HTML files from Web servers.

web browser an application program that provides a way to look at and interact with all the information on the World Wide Web. The word "browser" seems to have originated prior to the Web as a generic term for user interfaces that let you browse text files on-line. By the time the first Web browser with a graphical user interface was invented (Mosaic, in 1992), the term seemed to apply to Web content, too. A commercial version of the original browser, Mosaic, is in use. Many of the user interface features in Mosaic, however, went into the first widely used browser, Netscape Navigator. Microsoft followed with its Internet Explorer. Today, these two browsers are highly competitive and the only two browsers that the vast majority of Internet users are aware of.

World Wide Web all the resources and users on the Internet that are using the Hypertext Transfer Protocol (http). Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), http is an application protocol. Your Web browser is an http client, sending requests to server machines. When the browser user enters file requests by either "opening" a Web file (typing in a Uniform Resource Locator, or URL) or clicking on a hypertext link, the browser builds an http request and sends it to the Internet Protocol address indicated by the URL.

Cyber crime-specific terms

back door a hidden means of reentering a computer that a hacker or cracker can use if the original entry point has been detected.

buffer overflow a technique for crashing or gaining control of a computer by sending too much data to the buffer in a computer's memory.

cracker a hacker-for-hire who breaks into computer systems to steal information.

denial of service the result of hammering a web site's equipment with too many requests for information, effec-

TERMINOLOGY, cont'd

tively clogging the system and slowing performance or even crashing the site.

dumpster diving sifting through a company's garbage to find information to help break into its computers.

hacker generally, an individual with an affinity for computers. White-hat hackers are intrigued by the intellectual challenge of tearing apart computer systems to improve computer security. Black-hat hackers purposely crash systems, steal passwords, etc., not necessarily for financial gain.

insider an employee who works alone or with outsiders to compromise his or her company's computer system.

logic bomb an instruction in a computer program that triggers a malicious act automatically.

malicious applet a program that misuses a computer's resources, modifies files on the hard disk, sends fake electronic mail, or steals passwords automatically.

pagejacking appropriation of web site descriptions, key words, or links to draw consumers to a particular site which may be designed to facilitate unlawful activity.

password cracker a software program that can guess passwords.

scan widespread search of the Internet to determine types of computers, services and connections. Hackers and crackers scan to take advantage of weaknesses in a particular make of computer or software program.

script bunny a hacker with little technical savvy who is able to download programs—"scripts"—from rogue web sites or bulletin boards that automate the job of breaking into computers.

sniffer a program that covertly searches packets of data as they pass through the Internet, capturing passwords or the entire contents.

spoofing creating a false e-mail address or web page to trick users into passing along critical information like passwords or credit card account numbers.

social engineering a tactic used by hackers and crackers to gain access to computer systems by talking unsuspecting company employees or others out of valuable information, such as passwords.

trashing (see *dumpster diving*)

Trojan horse a program that appears to be harmless but actually contains instructions that exploits a known vulnerability in software.

virus a piece of programming code inserted into other programming to cause an unexpected and, for the victim, usually undesirable event. Viruses can be transmitted by downloading programming from other sites, or they can be present on a diskette. The source of the downloaded file or diskette often is unaware of the virus. The virus lies dormant until circumstances cause its code to be executed by the computer. Some viruses are playful in intent and effect while others can be quite harmful, erasing data or requiring hard disk reformatting.

war dialing launching a program that automatically dials thousands of telephone numbers in search of a way through a modem connection.

worm a type of virus or replicative code that situates itself in a computer system in a place where it can do harm. There are viruses that don't worm themselves into a place where they can do much harm and that replicate themselves via e-mail in many computers. Like most computer viruses, worms usually come in Trojan horses.

Selected References

Bowker, Arthur, and Thompson, Greg. "Computer Crime in the 21st Century: Its Effect on the Probation Officer" (unpublished manuscript, undated).

Brunker, Mike. "Mitnick goes free, but must remain totally unplugged." *MSNBC.COM* (Feb. 14, 2000) <http://www.msnbc.com/news/178825.asp?cp1=1#BODY>.

Committee on Criminal Law. *Model Search and Seizure Guidelines*. Washington, D.C.: Judicial Conference of the United States (1993).

Electronic Crimes Policy Team. *Cellular Telephone Cloning: Executive Summary*. Washington, D.C.: U.S. Sentencing Commission (January 2000).

Hafner, Katie, and Markoff, John. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Simon & Schuster, 1991.

Harrison, Ed. "Supervising the High-Tech Offender" (unpublished manuscript, 1998).

Lanning, Kenneth. "Cyber 'Pedophiles': A Behavioral Perspective." *The APSAC Advisor* (Winter 1998) (reprint).

Office of the Attorney General. *Cyberstalking: A New Challenge for Law Enforcement and Industry—A Report from the Attorney General to the Vice President*. Washington, D.C.: U.S. Department of Justice (August 1999).

Office of Education and Sentencing Practice. *2000 Amendments to the Federal Sentencing Guidelines*. Washington, D.C.: U.S. Sentencing Commission (undated).

Office of Juvenile Justice and Delinquency Prevention. *Use of Computers in the Sexual Exploitation of Children*. Washington, D.C.: U.S. Department of Justice, Office of Justice Programs (June 1999).

Policy Development Team. *No Electronic Theft Act*. Washington, D.C.: U.S. Sentencing Commission (February 1999).

President's Working Group on Unlawful Conduct on the Internet. *The Electronic Frontier: The Challenge of Unlawful Conduct Involving Use of the Internet*. Washington, D.C.: U.S. Department of Justice (March 2000).

Sager, Ira; Hamm, Steve; Gross, Neil; Carey, John; and Hof, Robert D. "Cyber Crime." *Business Week*, February 21, 2000: 36.

U.S. Sentencing Commission. *Report to Congress: Adequacy of Federal Sentencing Guideline Penalties for Computer Fraud and Vandalism Offenses*. Washington, D.C.: U.S. Sentencing Commission (June 1996).