Computer Crime in the 21st Century and Its Effect on the Probation Officer

Arthur L. Bowker, U.S. Probation Officer, Northern District of Ohio
Gregory B. Thompson, U.S. Probation Officer, Southern District of Indiana

IN TODAY'S TECHNOLOGICAL environment, the computer is becoming not only a beneficial aid for law enforcement, but the tool of choice for a new generation of offenders. Computers are now used to facilitate many traditional crimes, as well as new "cyber crimes." Two years ago, the typical computer offender was an employee taking advantage of an employer's computer system. More recently, "hackers" have manipulated the computer systems of the White House and the FBI, agencies whose security measures are among the best. As the 21st century commences, hacking and other computer offenses will become increasingly common. This requires law enforcement agencies and probation offices to be staffed with computer-literate employees. This article specifically addresses what probation offices can do to assist the courts in effectively supervising the computer offender. We also will suggest investigative techniques and possible special conditions for computer offenders. Finally, we will mention what steps the U.S. Sentencing Commission has taken in writing guidelines for computer offenders. As more computer criminals enter the probation offices across the country, it is evident that computer knowledge will be necessary. Probation officers must become computer savvy to keep up with the ever-changing offender.

Consider the following:

- A 30-year-old compulsive gambler, convicted of embezzlement, is placed on six months home confinement with electronic monitoring at his parents' home. This offender begins "surfing the net" on his father's computer and quickly locates numerous gambling sites. Unbeknownst to his parents or his supervision officer, he begins gambling in "cyber-space," which is a clear violation of a no-gambling condition imposed by the court.
- A 54-year-old male, convicted of receiving child pornography through the mail, secures employment at a large corporation. Although his computer experience is limited, he is allowed Internet access. Within a few weeks he begins "exploring" adult entertainment sites until he finally downloads child pornography.
- A probation officer is assigned a presentence investigation report on a defendant who "hacked" into a local airport's computer system. During the home visit, the probation officer notes an extensive computer system. What conditions can the probation officer recommend to the court? Do those recommendations change if the defendant relies heavily on that system in his employment?

To address computer offenders, probation officers need to develop unique investigative and supervision techniques to improve their ability to complete presentence investigation reports and recommend and enforce conditions, risk control, correctional treatment, and community protection.

Investigations

Although computers are a new instrument, probation officers need not discard their traditional investigative techniques. Traditional techniques, such as interviewing collateral contacts and examining records, are extremely important means of identifying problem areas. We believe such traditional techniques should be considered first before jumping into more technical and problematic areas of investigation. Interviews with third parties and the offender may reveal how the computer was misused during the offense or evidence that a computer or the Internet is being misused during supervision. Employer contacts can reveal that the offender has access to the Internet, or that a third-party risk exists. Interviews with family members and significant others can provide information on where, when, and for how long an offender is using the Internet. For instance, an interview with the mother of an offender who is prohibited access to the Internet may disclose that he began spending an enormous amount of time at the local library. A subsequent interview with the librarian may disclose that the offender has been admonished several times for exceeding the allotted time on the library's Internet computer. Moreover, knowing the time frame of use can narrow the scope of a computer system search when such a technical step becomes necessary.

Various forms of record examination can also be beneficial. Reviewing "hard copy" documents such as bills, telephone records, and computer printouts may reveal signs of computer usage or Internet access. Telephone bills may reflect billings for multiple lines into the offender's home, one of which may be used for a computer. A credit check, or credit card and bank statements may reflect Internet access charges, on-line debits/credits (indicative of Internet gambling), or large purchases at office supply or computer stores. Other records the officer can examine are sign-in

sheets or similar logs that may be maintained by employers, local libraries, or universities to record computer/Internet usage.

All officers should be aware that any documents provided by an offender are subject to computer manipulation and/or falsification. Probation officers should always look for possible inconsistencies over time in the documents provided by an offender. These inconsistencies may be signs that the documents are bogus. For instance, an offender, reportedly working for a sales company that employs over one hundred people, provides monthly pay stubs numbered 100, 115, and 110. It is highly improbable for a company of a hundred or more employees to have paid this offender with checks that are only a few digits off from one another over a six-week period. As is always the case, third-parties should be contacted to verify any information provided by an offender.

With the advent of technology, not only have the offenders been advancing, but so have the law enforcement professionals. For example, a number of software programs are available to monitor the computer activity of an offender. Examples of districts using computer monitoring and filtering programs to supervise certain computer offenders are the Southern District of Indiana, Middle District of Florida, the Southern District of New York, Western District of Texas, and the Western District of Wisconsin. Monitoring programs are designed to capture the sites an offender visits by either recording the sites visited and/or sending a screen snapshot every time the offender is on line. Filtering programs prohibit the offender's access to certain web sites. Some critics believe these software packages are too new to the probation field and need refining. One chief concern is that such programs can provide a huge influx of information needing to be reviewed on a regular basis, thus overloading the probation officer. Filtering software, on the other hand, has been criticized for not blocking what it is intended to block, as well as blocking sites it shouldn't. Additionally, there are numerous hacker sites that provide detailed information on how to overcome filtering software. Youths have been known to access these sites to circumvent parental controls. Such software programs are beneficial, but at this juncture they tend to be more advantageous for the less sophisticated user. The more knowledgeable the offender, the more likely he is to manipulate the program to his liking. As probation offices work with the software manufacturers, this may change (Collette, 2000).

Monitoring/filtering software should be considered as one supervision tool, but not the only one at the probation officer's disposal. A limited computer search should be used to insure the software has not been compromised by the offender. Additionally, the software or other sources of information may establish a "reasonable suspicion" that the offender has violated a supervision condition. The results of the monitoring software can then be used as a basis for a more intrusive computer search and/or seizure.

Supervision of Computer Offenders

Although the best condition for any computer offender may be no computer at all, there are three areas of concern regarding such a broad restriction. First, some argue that the term "computer" is becoming an increasingly difficult word to define. If a condition ordered states "the offender is to refrain from having access to a computer while on probation, unless authorized by the probation officer," the definition of computer is too general. Is a computer the CPU, the monitor, the scanner, the software, the keyboard, or is it also a pager, a cell phone, and a palm pilot organizer? Technology is advancing in that cell phones, pagers, and organizers have access to the Internet. What is allowed and what is not allowed?

Fortunately, there is some guidance on this first issue. Painter (2001) notes that Kevin Mitnick, a notorious hacker, argued before the District and Appellate Courts ". . . that broad conditions restricting access to computers are fatally vague and overboard." His argument was that computer chips are in everything from automobiles to toasters and that he would be forced to live like a hermit or commit unintentional violations of his supervised release. Both courts rejected this argument, noting conditions restricting computer access should be read in a commonsense manner. Painter cites the following court case to support this interpretation:

> [F]air warning is not to be confused with the fullest or most pertinacious, warning imaginable. Conditions of probation do not have to be case in letters six feet high, or to describe every possible permutation, or spell out every last self-evident detail [they] may afford fair warning even if not precise to the point of pedantry. In short, conditions of probation can be written-and must be read in a common sense way. *United States v. Gallo*, 20 F.3d7, 11 (1st Cir. 1994). (internal citations omitted) (p. 48)

The second concern with a no-computer condition is that computers are becoming a more integral part of everyone's lives. In one form or another, they are now found in every work and educational environment in the nation. Consequently, judges may not wish to prohibit all access to computers, so specific conditions regarding the Internet, bulletin board systems (BBS), and chat rooms may be more appropriate.

Finally, the no-computer condition typically includes the phrase "unless authorized by the probation officer." Such wording provides the probation officer the authority to either completely restrict or give authorization in certain circumstances. Absent appropriate training and/or court guidance, some probation officers may be inclined to simply deny any access without regard to the particular circumstances of a case. Such blanket denials may not always pass court scrutiny. Again, Kevin Mitnick tested his supervision officer's resolve. One of Mitnick's conditions directed that he was ". . . not [to] act as a consultant or advisor to individuals or groups engaged in any computer activity, as directed by the probation officer." In part because of his notoriety, many of Mitnick's employment offers involved computers. Mitnick did not first present the details of these offers to his probation officer for a decision. Instead he chose to proceed directly to the court, arguing that his probation officer had denied him the opportunity to work. The District Court concluded that blanket decisions were unacceptable without consideration of the specific offers. Since this decision, the probation officer reviewed the employment offers and Mitnick now writes, consults, and speaks on computer-related subjects. This is a prime example of a highly intelligent offender questioning the discretionary decision of the probation officer. When computers are essential to an offender's livelihood, it is likely that courts will follow what has occurred in the Mitnick case. Therefore, probation officers need to know how to supervise an offender who is allowed limited access to computers, or is allowed to be employed as a consultant to computer companies (AP, 2000).

To address these changing times and to avoid later difficulties, a probation officer must be qualified to conduct an educated assessment of a computer offender before he/she makes a recommendation for special conditions. Additionally, courts in the future may ask the probation officer what type of special conditions should be ordered in "high-tech"

cases. To answer such questions, we must be prepared to make an accurate and exhaustive assessment. Assessment entails obtaining and evaluating information about the offender and the offense to address a computer risk. Any assessment of computer risk must examine the conviction offense, the computer knowledge and ability of the offender, prior criminal conduct involving computers, the necessity of the offender having computer access, and the availability of a computer or the Internet. An accurate assessment of these factors will ensure that special conditions regarding access to a computer are in congruence with 18 U.S.C. §§ 3553, 3563, and 3583.

In the Mitnick case the Central District of California imposed some of the most restrictive computer conditions imaginable. However, these conditions were necessary in view of Mitnick's repeated history of committing high tech crimes. Mitnick had previously been on supervised release for a computer offense. He absconded from that supervision and became a fugitive committing additional computer offenses. Painter notes:

> In imposing the extensive conditions of supervised release, the judge held a number of hearings and based her ruling on defendant's long history of hacking, defendant's inability to comply with less onerous restrictions and, most importantly, the need to protect the public. The court's focus on the "tools" Mitnick has habitually used to commit past criminal conduct, computer and cellular phones, was wholly appropriate given defendant's seeming inability to use these tools in a law-abiding manner. Given his past extensive and repeated criminal conduct, and the prospect that, unsupervised, he would be tempted to engage in the conduct again, the court expressly stated that the conditions were designed to protect the community. . . . (pp. 45-46)

Table 1 provides some suggested computer conditions based upon the degree of computer/Internet access that is appropriate to a particular case.

A lack of special conditions regarding computer crime does not authorize the probation officer to neglect the offender's access to computers. As previously stated, computers are used to further many crimes outside of fraud and child pornography. Therefore, the probation officer still has many investigatory areas to develop in risk control and prevention. Simple techniques such as browsing a history icon or bookmarks can reveal evidence of violations for the less sophisticated offender.

More intelligent offenders may require more advanced techniques. They may also require more advanced conditions or special orders from the court. Most courts will not issue such an order without substantial evidence. We believe advanced forensic techniques are better left to those who have received the appropriate training in computer investigations and forensics. With the appropriate authority, the ability to search an offender's hard drive and locate hidden or erased files can provide valuable information on an offender's activities. Knowing how to download selective files and make a "logical copy" and a "mirror image" of a hard drive for later in-depth examination also facilitates the detection of illegal activity (See Table 2). More intrusive methods involve seizing the offender's computer for forensic examination by others.

Examining media storage devices (i.e., disks, hard drives, zip drives, tapes, etc.) is a very time-consuming task. Many of these devices can now store millions and millions of bytes of information. For instance, 1 gigabyte (GB), currently a small size in data storage, holds 1,073,741,824 bytes of information or the equivalent of a pickup truck filled with paper. Suggested time frames for searching a 3 GB hard driver are as follows: 3 kilobytes (KB) equals one page; 3 GB equals 1,000,000 pages. Time to review: 5 seconds/page, 12 pages/minute, 730 pages/hour, 17,280/day, total review 58 days. These time frames do not assume keyword searches or other techniques for narrowing the search (Bowker, 2001). Probation officers would be well advised to use traditional investigative techniques to limit the scope of their examinations as previously indicated.

Moreover, gaining access to an offender's computer at the workplace also presents difficulties for the probation officer. A work-site computer may be connected to a mainframe, a local area network (LAN), or a wide area network (WAN). In addition, there are obvious liability concerns for accessing a work-site computer, such as inadvertent damage to system. Because of these intricacies, gaining permission from the employer is a legal requirement.

Seizing a computer takes very specific skills and knowledge. Evidence can be lost by merely turning on the system without the proper procedures in place. The offender may also have "hot or test keys" that when struck activate programs that either destroy or encode data. There can also be civil and criminal penalties for improperly seizing a computer. These are just a few examples of things that might go wrong for someone who has little expertise in computer seizure procedures. *The Model Search and Seizure Guidelines* (Judicial Conference of the United States, March 1993) also discourages search and seizures. This policy statement, coupled with the technological complexities of computer evidence, make seizing a computer a last resort for a probation officer.

Use of the Computer by the Probation Officer

Although computers can facilitate crime, they can also assist officers in the investigative process. For instance, the Internet is a vast collection of information that is stored in hundreds of thousands of connected computers throughout the world. The Administrative Office of the United States Courts (AO) noted the following in its publication, *Internet Resources for Probation and Pretrial Services Officers* (1998):

> Probation and Pretrial Services Officers are called upon to collect personal data on individuals who are under bond consideration, pending sentencing, or under supervision. National telephone directories, street maps, and address locators are available on the Internet with easy to use graphical computer screens. Financial and social histories of individuals can be developed through on-line periodical searches. Current information (e.g. publications, articles, scholarly works) on substance abuse detection and treatment, mental health, and criminal justice are readily available.(p.2)

Cadigan (1998) noted several innovative uses of the Internet by probation officers. Specifically, probation officers have used the Internet to obtain information regarding street and prison gangs, militia groups, and "hate groups." Other officers have used the Internet to obtain information on the newest suggested techniques for defeating drug testing. One officer used the Internet to detect web pages developed by a sex offender with a special condition prohibiting him from using the Internet.

Siuru (1999) also reports the Internet is now being used by various courts to directly obtain information. Siuru indicates that G.T.E. Corporation has developed "The Bastille," an "Internet-based information-sharing service for law enforcement." The Bastille will permit the secure exchange of information between various law enforcement subscribers. Cadigan correctly predicts

TABLE 1
Suggested Computer Conditions

(A=Internet Access Permitted, B= Limited or No Access to Internet)	A	B
You shall consent to your probation officer and/or probation service representative conducting periodic unannounced examinations of your computer(s) equipment which may include retrieval and copying of all memory from hardware/software to ensure compliance with this condition and/or removal of such equipment for the purpose of conducting a more thorough inspection; and consent at the direction of your probation officer to having installed on your computer(s), at your expense, any hardware or software systems to monitor your computer use or prevent access to particular materials. You hereby consent to the periodic inspection of any such installed hardware or software to insure it is functioning properly.	X	X
You shall not possess encryption or steganography software.	X	X
You shall provide your probation officer accurate information about your entire computer system and software; all passwords used by you; and your Internet Service Provider(s).	X	X
You shall possess only computer hardware or software approved by your probation officer. You shall obtain written permission from your probation officer prior to obtaining any additional computer hardware or software or Internet Service Provider(s).	X	X
You shall refrain from using a computer in any manner that relates to the activity in which you were engaged in committing the instant offense or violation behavior, namely _____.	X	X
You shall provide truthful information concerning your identity in all Internet or E-Mail communications and not visit any "chat rooms" or similar Internet locations/sites where minors are known to frequent.	X	
You shall maintain a daily log of all addresses you access via any personal computer (or other computer used by you), other than for authorized employment, and make this log available to your probation officer.	X	
You shall not create or assist directly or indirectly in the creation of any electronic bulletin board, Internet Service Provider, or any other public or private network without the prior written consent of your probation officer. Any approval shall be subject to any conditions set by the U.S. Probation Office or the Court with respect to that approval.	X	X
You shall not possess or use a computer with access to any "on-line" computer service at any location (including employment or education) without prior written approval of the U.S. Probation Office or the Court. This includes any Internet Service Provider, bulletin board system, or any other public or private computer network. Any approval shall be subject to any conditions set by the U.S. Probation Office or the Court with respect to that approval.		X
You shall not purchase, possess, or receive a personal computer which utilizes a modem, and/or an external modem.		X
You will have an occupational condition that you can not be employed directly or indirectly where you are an installer, programmer, or "trouble shooter" for computer equipment.	X	X

TABLE 2
Basic Computer Retrieval Techniques

Downloading	Process of copying selected computer files. Process does not take much time.
Logical Copy	Copies all non-hidden files and non-hidden directories. Moderate amount of time involved, depending upon number of files/directories.
Mirror or Duplicate Image	Is an exact copy of everything, including hidden files/directories, data remaining from erased files/ directories. Also includes information from unused space. Moderate amount to extreme amount of time, depending upon the media being duplicated. Not unusual for new disk drives to take 12 or more hours, depending upon equipment used.

"as officers become more familiar with information that can be accessed through the Internet, it will play an increasing role in enhancing work practices and help officers 'work smarter, not harder.'"

Stored Wire and Electronic Communication

Probation officers must understand the statutes pertaining to e-mail and other forms of stored electronic communication. Federal law, specifically 18 U.S.C. §§ 2701-2771, provides for both criminal and civil penalties for anyone who accesses without or in excess of authorization a facility through which electronic communication services are provided, " . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while in electronic storage." Probation officers supervising offenders must not access any unopened e-mail or similar electronic communication in storage without specific authorization of the court or consent of the offender. E-mail that has been opened and saved to an offender's system is not covered by this provision. Some offenders may be providing e-mail services on their computer systems to other individuals. Under no circumstances should a probation officer access any e-mail or similar electronic communication in storage pertaining to other individuals without appropriate legal consultation and approval of the court.

Privacy Protection Act

Any offender with a computer, particularly one with a modem, can be considered a publisher within the meaning of the Privacy Protection Act (PPA), 42 U.S.C. § 2000AA. The PPA provides for civil penalties for anyone who seizes, without a subpoena, work products or documents that are intended for dissemination to the public. Work products or documents can be saved electronically in a computer. The following are general exceptions to this provision: information that is contraband or fruits of instrumentalities of the crime (i.e., child pornography, illegally copied software); information that is evidence of crime committed by the subject (i.e., diary confession to a particular offense); to prevent death or serious injury; subpoena has been tried and failed; or reason to believe that a subpoena would result in destruction of evidence. In *Steve Jackson Games, Inc. v. U.S. Secret Service* (1993), agents were found to have violated the PPA when they failed to return computers after it was learned they contained PPA-protected material. The plaintiff was awarded over $300,000 in damages, attorney's fees, and costs. As always, probation officers should obtain legal consultation when dealing with the PPA or stored electronic communications.

U.S. Sentencing Guidelines

In June of 1996, the U.S. Sentencing Commission reported to Congress on two broad areas involving computer use by offenders. The first dealt exclusively with violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030). This study found that approximately 60 individuals had been convicted of this statute. Their profile of the "typical offender" was noted as follows:

> . . . computer criminals tend to be somewhat better educated individuals who have less significant criminal histories than those convicted of other federal crimes...the typical computer criminal has not been a sophisticated user, but is, rather, likely someone with a pedestrian level of computer expertise who misuses his employer's computer system in committing his offense. (U.S. Sentencing Commission, Adequacy of Federal Sentencing Guidelines, p. 8)

This study concluded that no definitive assessment could be made on the deterrent effect of the existing guidelines on computer crime because of:

> . . . 1) an inability to determine how much computer crime was occurring before the guidelines went into effect, 2) the relatively small number (approximately 60) of the guideline convictions to date under the pertinent statute, and 3) the general difficulty of determining the deterrent effect of any criminal sanction. (U.S. Sentencing Commission, Adequacy of Federal Sentencing Guidelines, p. 8)

At the time, the Commission was consulting with the U.S. Department of Justice's Computer Crime Division on proposals to amend the guidelines to account for anticipated increases in computer crime. Note that the U.S. Sentencing Commission's findings were based *solely* upon cases of individuals convicted of violating 18 U.S.C. § 1030. We strongly suspect a great deal of computer offenders may be lost in such tracking devices because computer crimes may be prosecuted under other statutes. This is possible because the statutory maximum penalty for 18 U.S.C. § 1030 is typically five years (It can reach 10 and 20 years, but only if the computer data was restricted due to reasons of national defense or foreign relations.). Offenses involving computers are frequently prosecuted under other statutes carrying stiffer penalties. One example is 18 U.S.C. § 1344, bank fraud, which carries a 30-year maximum term of imprisonment.

The report further noted computer use is evolving rapidly. For example, although the overall numbers remained small, computer use in federal child pornography cases grew by 5 percent between 1994 and 1995. In response to congressional mandates, the Sentencing Commission also amended the guidelines to provide for a two-level upward adjustment for cases of child pornography involving computer use (See U.S.S.G. § 2G2.1 (b) (3), U.S.S.G. § 2G2.2 (b) (5), U.S.S.G. § 2G2.4 (b) (3)). (SOAC, p. 30).

Just four years later, in May, 2000, the U.S. Sentencing Commission sent new guidelines to Congress proposing much stiffer penalties for "high-tech" crimes. These guidelines have since taken effect. In some cases, the specific guidelines more than doubled the sentence for computer and other high-tech crimes. For example, an offender who used the Internet to meet minors and engage in sexual relations had a potential guideline range of 18 to 24 months increased to 41 to 51 months. Other guideline changes covered offenders who steal the identities of credit card users and make them available on the Web for widespread use. These guidelines increase the penalties from typically probation, to a prison term of 15 to 21 months. An increase in the guideline range for violations of copyright or trademarks online was also adopted. (United States Sentencing Commission, *Guideline Manual*, November 1, 2000, United States Sentencing Commission, *Supplement to the 2000 Guidelines Manual*; Brunker, 2000; and Fields, 2000.)

There is also some precedent for the application of the guidelines in computer crime cases. In *U.S. v. Petersen* (1998), 9th Circuit, an enhancement for special skill pursuant to U.S.S.G. § 3B1.3 was warranted for a computer "hacker," who hacked into several sites and manipulated the phone lines of a radio station to win a car being awarded by the station. The Appeals Court found that the lower court did not err in assessing the special skill enhancement, pursuant to §3B1.3. However, in *U.S. v. Godman* (2000), the 6th Circuit Appeals Court recognized that a special skill enhancement was not appropriate for a defendant who had no formal computer training and had used desktop publishing software from a local retailer to counterfeit

currency. The Appeals Court in this case concluded:

> At a time when basic computer abilities are so pervasive through society, applying §3B1.3 to an amateurish effort such as Godman's would threaten to enhance sentences for many crimes involving common and ordinary computer skills. The Guidelines contemplate a more discriminating approach. (p.3)

Additionally, recent changes to the Guidelines reflect that an enhancement under §3B1.3 is warranted for a defendant who de-encrypts or otherwise circumvents a technological security measure to commit a criminal infringement violation (United States Sentencing Commission, *Supplement to the 2000 Guidelines Manual*, p.54).

In *U.S. v. Hibbler* (1998), 6th Circuit, a five-level increase for distribution of child pornography was warranted for someone who traded child pornography on the Internet, even though they received no "pecuniary gain." In *U.S. v. Williams* (1992),10th Circuit, an enhancement for "more than minimal planning" was appropriate for an embezzlement occurring over six months and involving numerous computer entries.

Other case law exists on the appeal of special conditions by a defendant. In *U.S. v. Crandon*, (1999) 3rd Circuit, the district court ordered the following condition: "The defendant shall not possess, procure, purchase, or otherwise obtain access to any form of computer network, bulletin board, Internet, or exchange format involving computers unless specifically approved by the U.S. Probation Office." The defendant lured a 14-year-girl via the Internet to a remote location, engaged in sexual activity, and also took photos of the young girl. The appeals court upheld the condition, stating the lower court did not abuse its discretion in ordering the condition and concurred the defendant's conduct and protection of the community were appropriate reasons to order the condition.

Because of the uniqueness of these types of crimes, it will be the probation officer's job to inform the court of possible adjustments related to the offense and the use of a computer that are not already defined by specific computer enhancements. U.S.S.G. § 3B1.3. (Special skill) and more than minimal planning (in some chapter 2 specific offense characteristics) appear to be the adjustments/characteristics that are the more obvious for computer offenses. Other possible adjustments might relate to the use of a juvenile "hacker" by an adult (§3B1.4, Use of a Minor) and the obstruction

Table 3
Common Computer Crime Terms

Cloning	Term used to described the interception of legitimate electronic serial numbers (ESN), which are later entered into a stolen cellular phones to permit their use. (An ESN is a unique number assigned to each cellular phone that is transmitted each time the phone is used. ESN permits the phone to be used and billed accordingly.)
Cracker	A hacker who gains access and destroys data, completes some other destructive act to the system or profits in some manner from the access.
Encryption	Term used for hiding information in a secret code. For instance, encrypting a file so that it can not be read or interpreted until it is decoded. A file can be encrypted and then hidden inside another file (See steganography below). By doing so the very existence of the file is hidden and if detected it still cannot be interpreted until it is decoded.
Hacker	Originally coined at MIT in 1960's to refer to a computer expert. Now used to define individuals who gain unauthorized access to computer systems.
Hot or Test Keys	Performs certain pre-set security functions when touched that either make data inaccessible, unusable, or reverse the process to restore it. A "booby trap."
Logic Bomb	Software program that when certain factors are present will execute particular functions, i.e., the destruction of data or systems. One offender placed a logic bomb on a system that was designed to delete certain systems if his employer ever removed his name from payroll records.
Phreaker	Hacker who predominately gains access to telecommunication systems. (Note: Use of "Ph" is a play on the word phone, common in the hacker community)
Salami Method	Computer program used in embezzlement schemes to "slice" a small portion of the proceeds (i.e. $.01) from numerous accounts or payments and place those proceeds into the control of the offender.
Sniffer Programs	Software program that is placed on a computer system to surreptitiously function as an electronic wire-tap by intercepting the keystrokes and resulting system responses of users. The results are written as a file for later review to obtain passwords and account identification.
Social Engineering	Use of social skills to deceive others into disclosing information or providing services that an individual is not entitled.
Spoofing	The mimicking or counterfeiting of legitimate Internet protocol, frequently used to obtain information to gain unauthorized entry into systems.
Steganography	The science of hiding information in another medium. For instance, a child pornography image inside another image file. It is practically impossible to detect such a concealment.
Trojan Horse	Software program used to hide more nefarious or destructive programs.
Virus	Software program that "infects" other computers and takes over the system for a variety of functions ranging from minor manipulation of programs to wholesale destruction of systems and data. Virus "infection" is by someone either willfully or through negligence placing the program onto a system.
Worm	Software program that is similar to virus, with the exception that once created the program can self-replicate itself and "infect" other systems without someone actually placing the program on the system. Worms can attack networks.

of justice enhancements (§3C1.1) for offenders who use "hot keys" or "test keys" to destroy computer evidence (see Table 3).

Conclusion

The computer is becoming a weapon in the arsenal of the everyday criminal. Drug users are becoming more sophisticated by using computers to keep track of "customers," shipments, and money. Hackers are shutting down university computer systems, airports, and other systems, sometimes resulting in millions of dollars in losses and the threat of fatalities. As a new century begins, so does the problem of computer criminals for the probation and parole system. The training of officers in technical aspects of computer investigations and support software will become a vital part of an effective probation office. Many excellent training programs are now available through such organizations as SEARCH (http://www.search.org/, accessed 05/30/2001); the Federal Law Enforcement Training Center (http://www.fletc.gov/, accessed 05/30/2001); the High Technology Crime Investigation Association; (www.htcia.org, accessed 05/30/2001) and the National White Collar Crime Center (http://www.cybercrime.org/index.html, accessed 05/30/2001). It appears that as these problems become more prevalent, the necessity for some probation officers to become technical experts in computers will be inevitable.*

As criminals and their *modus operandi* change, so must the probation officer. We suggest officers who have the desire to excel in this area seek out training to become more educated in the computer arena. As the future unfolds, it may be common to have one or a handful of computer- literate probation officers specializing in the supervision of computer offenders. Not only can a computer-skilled probation officer supervise computer offenders, but he/she can also work in tandem with other specialists to further the effective supervision and investigation of all offenders.

As the 21st century commences, the supervision of computer offenders will become a common occurrence. The question for the probation field is whether we will be supervising them effectively due to preparation and training, or whether we will be attempting to catch up because we did not capitalize on the opportunity to address the issue earlier.

*Many offices across the country are also developing computer expertise. A few notable examples are: Southern District of Indiana, Middle and Southern Districts of Florida, the District of Columbia, Northern District of Ohio, and Western District of Texas.

References

Administrative Office of the United States Court, Federal Corrections and Supervision Division Center. (1998) *Internet Resources for Probation and Pretrial Services Officers*. Washington D.C.

The Associated Press (July 13, 2000). "Hacker Kevin Mitnick Allowed Back Online." www.nandotimes.com.

Bowker, Arthur (Spring 2001). "Providing a Frame of Reference: Lay Examples of Electronic Storage." *National Cybercrime Training Partnership Newsletter.*

Bowker, Arthur and Drinkard, Len (1996). "Downloading: Using Computer Software as an Investigative Tool." *FBI Law Enforcement Bulletin*, 65/6, 1-6.

Brunker, Mike (May 2, 2000). "Stiff Penalties Sought For Computer Crime." *MSNBC*, www.zdnet.com.

Cadigan, Timothy (August 3, 1998). "Officers Are Making Good Use of the Internet." *News and Views*. Administrative Office of the United States Courts, Federal Corrections and Supervision Division. 23(16).

Collette, Paul (April 24, 2000). "Monitoring Offenders' Internet Activity." *News and Views.* Administrative Office of the United States Courts, Federal Corrections and Supervision Division. 25(9).

Davis, L., McShane, M. & Williams, F.P. (1995). "Controlling Computer Access to Pornography: Special Conditions for Sex Offenders." *Federal Probation*, 59(2), 43-48.

Durkin, Keith (1997). "Misuse of the Internet by Pedophiles: Implications for Law Enforcement and Probation Practice." *Federal Probation*, 61(3), 14-18.

Fields, Gary (May 5, 2000). "Congress to Address Cybercrime Sentencing." *USA Today*, www.usatoday.com.

Painter, Christopher (March 2001). "Supervised Release and Probation Restrictions in Hacker Cases." *United States Attorney's Bulletin*, March 2001, Vol. 49, No. 2

Siuru, Bill (January/February 1998). "Tracking (or Trekking) Across the Internet." *Corrections Technology & Management,* 40-43.

Steve Jackson Games, Inc. v U.S. Secret Service, 816 F. Supp. 432 (W.D. Tex. 1993), aff'd, 36 F. 3d457 (5th Cir. 1994).

Stored Wire and Electronic Communication and Transactional Records Access, 18 U.S.C. §§ 2701-2771.

The Privacy Protection Act, 42 U.S.C. § 2000AA.

United States Attorney's Office of the Northern and Southern Districts of Ohio (1998), *Practical Problems in Searching and Seizing Computer.*

U.S. Parole Commission, *Procedures Manual* 28 CFR §2.40-22.

U.S. Sentencing Commission (1996). *Guidelines, News from the U.S. Sentencing Commission*, August 1996, 8.

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

U.S. Sentencing Commission (1996). *Report to Congress: Sex Offense Against Children, Findings and Recommendations Regarding Federal Penalties,* June 1996.

U.S. Sentencing Commission (1998). *United States Sentencing Commission Guidelines Manual*, November 1998.

U.S. Sentencing Commission, *United States Sentencing Commission Guidelines Manual*, November 2000.

United States Sentencing Commission, *Supplement to the 2000 Guidelines Manual.*

U.S. v. Crandon, 3rd Circuit, (1999), No. 98-5161.

U.S. v. Godman, 6th Circuit, (2000), Electronic Citation: 2000 FED App. 0261P (6th Cir.)

U.S. v. Hibbler 1998, Electronic Citation: 1988 FED App. 0317P (6th Cir.).

U.S. v. Mitnick, Central District of California, Case Nos. CR-603-MRP and CR 96-881-MRP.

U.S. v. Petersen, 1998, 98 F. 3d 502.

U.S. v. Williams, 1992, 966F.2d555,558-59, 10th Cir. 1992.

Wang, Wallace, *Steal this Computer Book: What They Won't Tell You About the Internet*, (San Francisco: William Pollack, 1998)