Supervising the Cyber Criminal

Brian J. Kelly
Senior U.S. Probation Officer and Cybercrime Specialist

ENACTED IN 1986 and amended several times since then, 18 USC 1030, the Computer Fraud and Abuse Act, is the primary criminal statute used for prosecuting fraud and related activity in connection with computers. This statute covers those who knowingly and/or intentionally access a computer(s) and obtain information they were not authorized to have access to.

As the world of computers and cyberspace becomes more and more ingrained into our daily lives, so will cybercrime. Increased prosecution of cybercrime will mean, for United States probation officers, preparing for the special demands of efficiently investigating and supervising these offenders and providing the court with understandable and accurate information about them.

First, who is the cybercriminal? He or she is not simply the lone juvenile hacker using a Christmas present from Mom and Dad. Cybercriminals come in all forms, from the street drug dealer to the identity theft mastermind. Many people place in this group the sexual predator who makes use of a computer for child pornography and solicitation. In my opinion, these offenders belong in a different category from those we are discussing in this article. Sexual predators' computer use is secondary; their problem is deeper rooted. Take away sex offenders' computers and they will, if they have not already, find other ways of luring children, distributing and receiving child pornography, etc. The focus of the supervision of the sex offender should be the offender's mental state and ability to carry out desires. (Sex offender and cybercrime specialists will, however, have much in common and are likely to work in tandem at times as cyberspace increasingly becomes the means of choice by sex offenders.)

The cybercriminal can be defined as someone whose knowledge and use of computers and/or the Internet has enabled him or her to commit the crime of choice. This definition covers everyone from the first-time offender whose spontaneous hack into a former employer's database is based on revenge to hacker/crackers such as Kevin Mitnick, who have a long list of computer-related offenses and whose instant offense is the culmination of criminal activity covering a period of months or even years, spanning intrusion into classified military information to obtaining free telephone service.

The Pre-Sentence Interview and Report

The first duty of the United States Probation Department is the preparation of the Pre-Sentence Report, which contains a sentencing recommendation to the court. For the cybercriminal, the PSR must contain a clear and precise offense conduct section explaining the motive and means of the offense. The court and, eventually, the supervision officer determine the offender's computer knowledge and motive for participation in the offense. The motive may be purely financial (intrusion into an e-commerce web site to steal customer information, for example), anger (denial of service attack on a former employer), or extortion (intrusion into an e-commerce web site to steal information to use to extort the company instead of further criminal use). The report should also accurately describe the computer equipment owned by the offender. Most important, the report carries a sentencing recommendation to the court. This recommendation must include specific special conditions covering the offender's computer and Internet usage. How restrictive these special conditions should be is based on the severity of the instant offense and the offender's criminal history. For example, a first-time offender who has committed an isolated denial of service attack against a former employer may not warrant a full prohibition from computers and/or the Internet but rather a condition prohibiting any contact, including computer contact, with the former employer, as well as employer notification if the offender plans to obtain employment within the computer industry.

The Eastern District of New York Probation Department has recently issued a Bench Guide to the Judges of the district which includes the classification and wording of special conditions. The following are a few of the special conditions listed under the section titled "Cybercrime (Computer/Internet)":

- The defendant is not permitted to access a computer or a connected device (except a land line telephone) at any time.
- The defendant is not permitted to access the Intranet/Internet or bulletin board systems at any time.
- The defendant is not permitted to engage in the use of encryption.

Other special conditions should also be considered in these cases; for example, restitution for any damages caused by the offender, mental health treatment for anger management, search and seizure condition, etc.

Supervision Methods

Effective supervision of the cybercriminal need not be limited by the level of computer knowledge and skill of the officer. In fact, only a small percentage of the supervision of the cybercriminal will involve advanced computer knowledge. The majority of the supervision will combine traditional and non-traditional supervision methods with a level of computer knowledge consistent with regular use of a computer and the Internet. Considering the influx of computers into our professional and personal lives, this is not a steep hill to climb.

Officers supervising cybercriminals, and especially those who need to enforce cyber-specific special conditions, should become familiar with various methods that can assure full compliance and detection of non-compliance.

The Initial Interview

Using the pre-sentence report as a background, the cybercriminal should be interviewed with the same goal as with any other offender—that is, to obtain as much relevant information as possible. For cyber-specific information, the officer should attempt to gather two groups of information, addressing ability and means. Under the category of ability, how complex was the instant offense? What formal computer education/training has the offender had? How long has the offender been employed in the computer industry? As for means, what computer equipment does the offender own or have access to? Who are the offender's Internet Service Providers (ISPs)? What are the offender's email addresses/screen names? As previously stated, the pre-sentence report should contain a full listing of the offender's educational and employment history, as well as asset information.

In the Eastern District of New York, we have compiled a Computer/Internet Data Sheet for the offender to complete and return to the supervising officer. This Data Sheet contains questions about hardware, software, and Internet accessibility and use.

The Home Contact

As with any offender, the home contact is the most valuable supervision method, because it offers the officer an insight into the daily life of the offender. With the cybercriminal, the focus will mainly be on the computer workstation. Any evidence of non-compliance will most likely be found in this area. The officer should be familiar with the hardware the offender has reported he owns or has access to (*Computer/Internet Data Sheet*). Any hardware not listed or recently obtained should be recognized by the officer. The officer should be aware of any print-outs or notes in plain view around the work station. If the computer is on, the officer can note the software that may be running and other programs on the system by simply looking at the screen. During the home contact, the officer should also notice other connected devices, such as laptop computers, personal data assistants (PDAs, i.e. Palm Pilot), cellular phones, and pagers. The officer must be sensitive if the offender is living with other members of his/her family, since they may use the computer or other devices.

The Employment Contact

During the employment contact, officers should observe the offender's work area. Does the offender have access to a computer? Does the computer have Internet access? Is the computer networked with other computers? If possible, speak with the offender's supervisor to determine what kind of access the offender's daily duties make possible. The Internet? Other computers? Other databases?

Surveillance

An officer may deem it necessary to verify the daily activities of the offender to assure compliance with special conditions, such as prohibition from accessing the Internet. Surveillance of an offender's visits to locations such as the library, a "Net Café," etc., may indicate the offender is accessing the Internet at locations other than the residence.

Credit Reports and Card Statements, Telephone Records, Mail Covers

An officer should periodically obtain credit reports for the offender and request statements for any active credit cards from the offender. These statements may show charges that would provide insight into the offender's Internet usage, such as an ISP monthly charge, e-commerce purchase, or the like. Telephone records obtained from the offender may reflect calls to ISPs or other databases the offender is accessing with a dial-up modem. Mail covers, which can be requested from the U.S. Postal Inspection Service, can reveal incoming mail from ISPs, online trading accounts (i.e., E-Trade), or credit card companies. Mail covers are particularly useful if the offender is receiving mail using an alias. If warranted, credit card statements and telephone records can be obtained by a court order instead of by requesting the information from the offender.

A recent violation filed in the Eastern District of New York involved an offender obtaining names and social security numbers through stolen mail and using this information to establish fraudulent instant credit accounts online and purchase goods. The offender used his home address, on which a mail cover had been initiated by the officer, and incoming mail showed the names fraudulently used by the offender. This conduct resulted in violation proceedings as well as a new indictment within the district.

Random Hard-Drive Search

If the officer deems it appropriate and necessary, he or she may conduct random hard drive searches of an offender's computer. If no search special condition is in place, the officer must first gain the offender's consent to a search. The search can be as simple as a peripheral search during an unannounced home contact or as complex as physically taking the equipment from the offender and bringing it to a computer forensic lab for analysis. Of course, the removal of equipment from an offender's home or place of business should only take place in an extreme circumstance, where the officer must be prepared to deal with a variety of issues such as chain of custody, privacy laws (if the computer is accessed by other members of the family), etc. But basic peripheral searches that do not involve the removal of equipment, unless evidence of violation or new criminal conduct is uncovered, should be a practice of officers supervising cybercriminals. The following supplies should be on hand if such a search is planned: camera, floppy disks, labels, and note-taking materials. Before conducting a search, the officer should photograph the work station. The search can be done in two ways. First, the officer can enter the hard drive manually, searching folders such as Temporary Internet Files for evidence of Internet use and Notepad or Word documents for evidence of fraud (social security & credit card numbers, etc.). Obviously, this method takes a certain level of computer skill first to access the data and then to preserve it for evidence, if necessary.

If the officer's skill is limited or he/she does not feel comfortable manually searching the hard driver, software is available that will search for certain types of documents. In the Eastern District of New York, the Probation Department has previously used *One Tough Computer Cop,* a program originally designed for parents to monitor their children's computer use. The program is extremely simple to use and requires little computer knowledge.

Essentially, the program searches the hard drive for graphic documents (.bmp, .jpg) and text documents containing key words relating to drugs, violence, gambling, etc. The user can view selected documents easily and quickly. Recently, the company that designed *One Tough Computer Cop* introduced similar software specifically designed for probation and parole officers. EDNY has purchased *Computer Cop Forensi,* which operates on the same premise as *One Tough Computer* Cop but at a much more advanced level. The officer can install the software onto a laptop and via a parallel port cable can view and seize evidence from an offender hard drive while maintaining evidence integrity. This enables searches to take place in the field or in the office if a system is seized. Also used in EDNY are *Internet History Viewer* & *File Rescue.* To find the software that fits your district's particular needs, simply search the web.

During the search, the officer should make notes of any pertinent information, such as software on the hard drive, file information, etc. Once the search is completed, the officer should again photograph the work station.

If the officer deems it necessary to seize the hard drive, labels should be used to identify all hardware and connection ports. An excellent guide to the seizure of electronic equipment, entitled "Best Practices for Seizing Electronic Evidence," is available through a joint project of the International Association of Chiefs of Police and the U.S. Secret Service.

Officers should become familiar with legal issues surrounding the search and seizure of computers and electronic evidence. The Electronic Communications Privacy Act and Privacy Protection Act are two main pieces of legislation that officers should review. As United States probation officers, we have more leeway than other law enforcement agencies, but this should not be used as an excuse to be un- or ill-informed on legal issues surrounding any actions you may be planning to take. The Department of Justice web site on cybercrime (www. cybercrime.gov) contains a wealth of information on cybercrime, including legal statutes and case law.

Monitoring/Recording Software

In current use in sex offender cases are monitoring/recording software programs such as SpectorSoft. This program is installed onto an offender's computer to maintain a photographic record of the computer activity. The officer can randomly access the program and retrieve the data to determine if a violation has occurred or if the program has been tampered with.

Information Databases

The Probation Department currently has access to many information databases, such as Choicepoint, Lexis-Nexis, Westlaw, and SENTRY. All of these databases are extremely useful for obtaining information on offenders. When searching for information about a cybercriminal, officers should be aware of any hacker aliases the offender may have used. Many hackers find the need to brag about their exploits and conquests on message boards, and a random search may uncover such a message. If an offender obtains employment with a company that maintains a web site or claims ownership of a web site, or if the officer uncovers a domain name linked to the offender, the officer may search the **WWWHOIS** database. This database maintains owner information, including addresses and telephone numbers, for most domain names.

Recently, in the Eastern District of New York, an offender claiming to work for an employment agency provided the officer with the company's web site address. The offender, who owes a considerable amount of restitution, claimed to be the office manager, with no ownership interest or ties to the business. A search of the WWWHOIS database via www.network-tools.com revealed that the domain name was owned by the offender's husband and a listed billing address was a former residence of the offender.

Mental Health Evaluation & Treatment

Some cybercriminals are not out for profit but commit the instant offense out of anger, obsession, etc. These offenders should be referred for a psychiatric evaluation to ascertain the necessity for treatment. A spontaneous denial of service attack on a former employer may indicate a deeper anger management issue, while some offenders may have lost touch so completely with reality that they feel the only reality lies within cyberspace. These and other issues may require mental health treatment to prevent a "relapse" into further offense conduct as well as to prepare the offender for a functioning life outside of cyberspace.

The extent to which each of the above methods is used should be decided on a case-by-case basis, considering many factors, especially the restriction level of court-ordered special conditions.

Networking

Federal, state, and local law enforcement agencies have been identifying and addressing the threat of computer-related crime by forming cybercrime investigative units within their agencies. Some agencies have also put together their own computer forensic labs to perform in-house analysis of suspect computer systems. Making contact with these units is essential to the successful supervision of cybercriminals. The High Technology Crime Consortium and New York Electronic Crimes Task Force have put together listservs with Yahoo Groups for law enforcement and private industry professionals involved in the investigation of cybercrime and other technology-related issues. The list of members grows daily and anyone needing assistance in this field is greeted with a wealth of information from members.

Law Enforcement Task Forces are also an excellent way to make contact with other law enforcement professionals and gain assistance in an investigation. The New York Electronic Crimes Task Force coordinated by the U.S. Secret Service combines law enforcement and private industry to help combat cybercrime and other electronic crime.

Conferences such as Cybercrime 2001 Conference & Exhibition, International Conference on Electronic Crime, and Blackhat offer great opportunities to meet professionals in the computer industry and law enforcement professionals specializing in this area. Private companies that participate in these conferences demonstrate software products designed for information security and forensics. Officers should attend these conferences to keep up with the latest software offerings.

Officers should also become aware of legal contacts and subpoena procedures of Internet Service Providers. Obtaining records from ISPs may be the key to an ongoing violation investigation. A list of ISP legal contacts can be obtained at www.infobin.org/cfid/isplist.htm.

The most challenging aspect of cybercrime is the speed of change. Between the composing and publishing of this writing, new products have been released, new web sites formed, new crimes committed. Officers who plan to specialize in cybercrime must be prepared to stay constantly on top of current events. In the Eastern District of New York, cybercrime training has been incorporated into the new officer training program. The training sessions cover topics such as electronic databases, cybercrime special conditions, supervision methods, cybercrime statutes, forms, and media publications. Districts should seriously consider implementing cybercrime training and district policies in the near future to avoid playing a constant game of "catch-up" with the offenders they are supervising.