Cyber Crime and the Courts—Investigating and Supervising the Information Age Offender

Lanny L. Newville
Field Automation Specialist, Western District of Texas

"It should come as no surprise that computer technology is involved in a growing number of crimes. In addition to being used as a tool to perpetrate crimes (e.g., computer intrusion, stalking, harassment, and fraud), computers can contain evidence related to any crime, including homicide and rape. It is no longer sufficient to have a few experts familiar with evidence stored on and transmitted using computers. Any investigation can involve computers or networks and everyone involved in a criminal investigation or prosecution can benefit from knowledge of the associated technical, legal and evidentiary issues related to this technology."

—Eoghan Casey, Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet (Academic Press 2000)

BEFORE THE ADVENT of the Internet and the boom in communications it engendered, computer crimes were fairly localized and the perpetrators were members of a select and secretive group with a high degree of specialized knowledge and skills. The child pornography industry, which had already begun to move from print and film media to computer bulletin board systems, found an open and anonymous home on the Internet with a rapidly growing victim pool. According to Grunwald Associates, a research firm based in California, our children's use of the Internet has increased from 2.3 million in 1994 to 25.4 million in 1999.[1] Unfortunately, preferential sex offenders recognized the apparent advantages of the Internet and were well established before law enforcement became aware of the changes.

The Internet has allowed an explosion of information, both positive and negative. In addition to globalizing adult and child pornography, it has created a venue for the criminally oriented to freely exchange information and provides them with distance-learning opportunities to enhance their illegal skills. It is quite simple to find sites on the World Wide Web where step-by-step instructions for remotely breaking into computer systems, and stealing services such as long distance, and circumventing security measures are openly available. It can also serve as a support system for defendants who are looking for others to validate their behavior.

Those charged with investigating and apprehending violators have found themselves with a huge knowledge deficit. The FBI, U.S. Secret Service, and U.S. Customs have led the field in training investigators and forensic computer specialists. These agencies have made significant progress in their ability to detect and apprehend suspects, but the celerity with which computer technology is changing and the exponential increase in related criminal activity is broadening the gap. "In FY 1998, the Federal Bureau of Investigation opened 547 computer intrusion cases. In FY 1999, that number more than doubled, with a total of 1154 cases opened. In spite of increases in their ability to close cases, the FBI is realizing a rapidly increasing computer-crime-related caseload. The number of pending cases increased from 206 at the end of FY 1997, to 601 at the end of FY 1998, to 834 at the end of FY 99, and to more than 900 as of March of 2000. These statistics include only computer intrusion cases, and do not account for computer-facilitated crimes such as Internet fraud, child pornography, or e-mail extortion."[2] The U.S. Secret Service and the U.S. Customs Service have realized similar increases in this type of crime.

Additionally, the financial losses being attributed to computer crimes are staggering. The Computer Security Institute released the results of its 6th annual computer crime and security survey on March 12, 2001. Losses reported by 186 of the 538 respondents totaled more than $377 million, an increase of over $100 million from the losses reported by 249 respondents in the 2000 survey. Theft of proprietary information and financial fraud accounted for the largest proportion of loss. The respondents reported across-the-board increases in external system penetrations, denial of service attacks, and virus "infections." Surprisingly, only 36 percent of the respondents reported the intrusions to law enforcement authorities.[3]

Cyber crime poses a daunting challenge to the federal judiciary. While the majority of cases we investigate and supervise are related to the manufacture, distribution, and possession of illicit drugs, case filings involving the use of computers to commit or further a crime are on the increase nationwide.

With rare exception, our system has been slow to embrace technology and is far from able to boast a seat at the cutting edge of technology. We are being asked to supervise and protect the community from a new breed of defendants and offenders (referred to as defendants for the remainder of this article) who not only embrace technology, but also are finding increasingly sophisticated methods to use that technology to further criminal endeavors. We are seeing a phenomenon in which many traditional crimes are being committed using computers. When this activity takes place across the Internet or through the use of telecommunications, a nexus is present to bring it to federal prosecution and hence into our purview. Another phenomenon of the rapid growth in computer technology and the Internet is that larger numbers of juveniles are entering the system, and being charged with an array of crimes that were traditionally attributed only to adults.[4] The numbers have increased to the extent that legislation was introduced in 2000 seeking to make it easier to prosecute juveniles federally.[5] Other than anecdotal information pointing to escalating numbers of cases being investigated and supervised, we have no organized way to track the totals of computer-related or facilitated crimes in our existing statistical environment. We can only surmise that the number of cases that come under the supervision of the courts closely matches the number of prosecutions initiated by the U.S. Attorney's Office.

Like our law enforcement counterparts, we are not prepared to meet the challenge these defendants pose and must begin to develop methods to effectively supervise and enforce the supervision conditions imposed by the Courts. Only a handful of pretrial services and probation officers throughout the country have the knowledge and experience in technology to even begin to come to terms with some of the issues being raised. Even fewer have recognized this and begun the process of obtaining specific training to facilitate supervising these defendants.

To begin addressing the issues raised by these defendants, we must embark on a developmental process to raise the skill levels of our officers and automation staff to assist us in meeting the challenges supervising persons charged with computer crimes are placing before us. Several areas need to be targeted, including the identification and development of the following:

- Training in investigation methods (including computer forensics and interviewing skills).
- Adoption of the Judicial Conference's Model Search Policy (for those districts that will allow computer-related searches).
- Model wording for computer-related conditions of release.
- Supervision strategies.
- Purchasing computer software tools for tracking and monitoring defendants' activities if they are allowed to use a computer or access the Internet.
- Purchasing specialized hardware to detect and retrieve evidence of violations of release conditions on the defendant's computer.
- Providing training for officers tasked with supervision of these defendants.
- The creation and funding of a forensics laboratory to assist districts with investigations and training.

The course of action the system takes will largely depend on the latitude granted to us by the bench, especially regarding any actions that would fall under the broad umbrella of search authority, which is a supervision tool that traditionally has not been widely used.

Investigation Methods

Investigating "high-tech" defendants should not require the development of a workforce of super computer-literate "Cyber Geeks." What is necessary for officers performing investigations is to acquire a familiarity with the computer-related terminology and to develop a basic understanding of how the defendant is alleged to have used a computer to further or commit the offense. Through training, the officers' awareness will be raised and a level of competency will be established to ensure the integrity of the information we gather. This is very similar to training officers to a level of competence regarding substance abuse issues. Officers do not have to become therapists to effectively gather information, make an accurate assessment of need, and provide the courts with recommendations for responsive conditions to deal with identified problem areas. The Federal Judicial Center took the lead in this education process by developing a Special Needs Offender Series installment on Cyber Crime, which aired on the Federal Judicial Television Network on September 21, 2000.

The most important component of an effective investigation begins with a thorough interview. The insertion of technology into the process does not change the dynamics of effective interviewing techniques. As with any good interview, questioning should lead from general to specific detail and focus on open-ended inquiries. When possible, the officer should attempt to speak with a case agent or the Assistant U.S. Attorney to get information about the charged offense and how computers were involved. Armed with that information, the officer can focus in on pertinent questions to determine areas of risk that may need to be addressed through the imposition of a special condition. The officer should gather as much relevant information from the defendant as possible related to his use of computers, at home, school and/or work. Additionally, information about the type of computer and operating system, as well as what devices may be attached to the computer, who besides the defendant has access to the computer system, and what type of external connectivity the system has, may prove useful to the supervising officer.

These defendants are often very proud of the technology they employ and may tend to give more information than is necessary. It is also possible that they will attempt to befuddle the interviewer with jargon. Having a basic understanding of computers and technology will prepare the officer to deal with this and keep the interview on track. Pretrial services officers need to be wary of steering the questions too closely to offense-specific behavior. Probation officers, on the other hand, may need specific information regarding offense behavior to determine, for example, if guideline enhancements for special skills (U.S.S.G. § 3B1.3) should be applied.

Conditions of Release

The conditions of release for bond, probation, and supervised release are the nuts and bolts of the supervision process. Carefully crafted wording can prove invaluable in assisting the officer in restricting behavior, protecting the community, or providing resources for correctional treatment. Poor wording often leaves room for interpretation, provides defendants opportunities for manipulation, and can be the source of great embarrassment in court settings.

The list of computer-related crimes confronted for investigation and supervision purposes is both varied and constantly changing. The dynamic nature of the law in this area and the continuous advances in technology are making the job of drafting conditions more difficult. In 1999, a working group of probation and pretrial services officers, staff from the Federal Corrections and Supervision Division, and the Federal Judicial Center (FJC) was established to consult with the Federal Judicial Center for the development of their Special Needs Offender Series installment on Cyber Crime. The group's discussions, with guidance from the Office of

General Counsel, led to the development of several items that can be used as guidelines for the development of wording for conditions of release. These were contained in the Special Needs Offender Bulletin, *Introduction to Cyber Crime*, published by the Federal Judicial Center in August of 2000. Another good resource article specific to special conditions for sex offenders by Davis, McShane, and Williams, was published in the June 1995 issue of *Federal Probation*.[6]

We must keep in mind that the number of "new" computer-related offenses (i.e., Denial of Service and Computer Intrusions) being committed by these defendants is relatively small. The majority of cases being filed concern offenses we are very familiar with, but with the added twist that the crime was either perpetrated primarily through the use of a computer or furthered in some way by using computer technology. Examples of these offenses include counterfeiting of monetary instruments and other documents, embezzlement, fraud, drug dealers who store their distribution information or "recipes" on computer media, child pornography, etc. Inasmuch as these offenses are familiar to us, we should be reminded that traditional investigation and supervision methods are still valid. The time-tested conditions of release we have used continue to be legitimate.

When recommending computer-related special conditions of release, the officer should start from the premise that governs decisions for other conditions. Pretrial services officers must determine whether or not the condition 1) addresses a nonappearance issue; 2) addresses an issue of danger to the community or the defendant; and 3) is the least restrictive measure available to assure appearance and negate possible dangerousness. Probation officers recommending conditions should determine if the conditions being considered serve to reduce risk and/or provide correctional treatment. Consideration should also be given to minimizing the amount of intrusion monitoring of the condition will cause in the defendant's life, and reasonably relating the conditions to the offense charged and the defendant. The imposition of a condition prohibiting access to pornography-related web sites may make perfect sense when the offense is related to child pornography or traveling across state lines for the purpose of engaging in sex with a minor. Imposing a similar condition on someone charged with a computer-related fraud would be difficult to justify.

An officer's viewing or monitoring activity and/or logs from a defendant's computer may constitute a type of search. Conditions that allow this activity should not be imposed unless the district has implemented a search policy and is willing to undertake training officers and possibly automation staff to review and retrieve evidence of violations from computers and other digital media. Although we do not have to meet the evidentiary standards imposed on law enforcement agents to prove violations, information collected by officers without authority or in a way that places its authenticity in question may be useless in a violation hearing. This might become especially important if an officer's examination of a computer turned up what appears to be evidence of new criminal activity.

Conducting examinations of a defendant's computer can involve the use of a range of fairly simple software to a combination of sophisticated hardware and software applications. Conditions recommending the use of software tools should be worded based on the experience and ability of the supervision staff conducting the monitoring, as well as the level of computer knowledge and skills the defendant possesses. There are many commercially available programs professing the ability to block access to questionable sites on the Internet that can be easily defeated by persons with minimal computer skills. This is not to imply these "blocking" programs should not be used, but that their limitations should be understood before supervision or accountability problems arise as a result of their use.

Our ability to track or monitor computer use is largely dependent on the presence of information in computer log and history files and system cache directories. There are a number of software programs available that will allow a user to either encrypt or delete this information, thus making it difficult or impossible to retrieve. When recommending special conditions, then, thought must be given to prohibiting the defendant from using software and other technology designed to hide or remove the signs that they have done something to violate their conditions or the law.

A brief outline of computer-specific conditions that could be recommended to the court includes:

- No computer use or access at any location.
- No use of any device capable of accessing the Internet or an online service (i.e., Palm Pilots, Internet Capable Digital Phones, etc.).
- No Internet or Electronic Bulletin Board (BBS) access.
- Provide telephone / Internet service provider billing records monthly.
- Disclose all online accounts, including user-names and passwords.
- No access to modem or other connective device.
- No use of encryption technology or software designed to delete computer log files.
- Require the use of filtering software.
- Use of activity tracking and reporting software.
- Computer search / inspection condition.
- Provide a software/hardware audit at onset of case.
- No new hardware/software added to the computer without officer authorization.

This is by no means a complete list of conditions that could be imposed to address computer-related concerns. Other conditions, including electronic monitoring, third-party risk notification, mental health treatment, and travel restrictions may also be necessary to address identified issues.

Supervision Issues

The increase in case filings at the federal level during the past few years have provided demographic information that is allowing law enforcement agencies to develop a "profile" of defendants. Pretrial services and probation officers across the country report that the three primary groups that are coming into the federal system are: 1) "hackers"; 2) sex offenders who are using the Internet to meet and groom their victims or trade in child pornography; and 3) the traditional criminal defendant who has used computer technology to assist in the commission of a traditional offense such as counterfeiting or fraud.

The demographics suggest that most defendants charged with computer hacking and intrusion-related crimes generally range in age between 15 and 45 years old, are primarily male, and have little or no prior criminal record. They tend to work alone, but like to boast to their peers about their accomplishments (exploits). They are highly motivated and may tend to be manipulative and passive aggressive in authoritative confrontations. Officers supervising defendants in this group need to be mindful that they will tend to try to obscure information about their personal lives and want to engage in game playing. The officer may be able to take advantage of their love of games and challenges to encourage compliance. These defendants tend to make detailed lists regarding their activities and it would not be uncommon for the lists to be located on the computer or other electronic media.[7]

Defendants being charged with child pornography-related offenses and those charged with traveling across state lines for the purpose of engaging in a sex act with a minor do not fit into a specific demographic profile. The FBI has developed broad classifications for these offenders based on the work of now-retired Special Agent Kenneth Lanning. The classification of offenders most likely to fall under federal supervision is the "Fixated" or "Preferential" sex offender. This classification encompasses individuals who have a specific sexual preference for children and who seek out opportunities to act on their preference. They are highly compulsive, have difficulty forming sexual relationships with age-appropriate peers and often never marry or else enter into relationships of convenience as a cover for their behavior. Their pursuit of victims is carefully planned and they tend to form tight networks within which they trade victim-grooming techniques and trade child pornography.

The second classification is the "Regressed" or "Situational" sex offender. Individuals who fall into this classification may experience a sudden preference for children that coincides with major life stressors including adult relationship or career problems, and alcohol or drug addiction. Members of this group may have a history of relationship problems, and although they become attracted to children, are not necessarily primarily aroused by them.

These defendants, once charged, tend to be mostly cooperative with law enforcement and court-ordered supervision. However, because they are very compulsive in seeking gratification, supervising officers need to remain aware that many will continue to engage in behaviors that may be illegal or dangerous. This increases the risks of home and field supervision. Officers must also keep in mind that these defendants may become suicidal when their behavior is exposed, especially those who have established respectable, usually middle-class "covers" in their daily lives.

These defendants' compulsivity may also work to the advantage of officers monitoring their computer use because they frequently keep diaries of their activities and do not employ sophisticated means to hide their pornography collections. An offender under supervision in the Middle District of Florida is a prime example. The supervising officer received information that the offender might have been engaged in child pornography-connected behavior again. The officer sought and received approval to conduct a search under the district's search policy. During an examination of the offender's computer, the officer located a diary in which the offender had been chronicling his abuse of a number of minor children in the area. Law enforcement was notified and the defendant was eventually charged with a new offense and his release was revoked.

Aside from the specific characteristics of these defendants and the issues arising from their use of technology, officers should find that traditional supervision techniques are effective in gaining and monitoring compliance with conditions. Requiring them to provide documentation of employment, utility billing records, credit card records, and service agreements are a few examples. When practical, enlisting the assistance of family members, employers, and treatment providers will prove invaluable adjuncts to officer supervision.

Computer-Related Searches

Computers can play three distinct roles in a criminal case. A computer can be the target of an offense when the confidentiality, integrity, or availability of its information or services is attacked. Computers can be incidental to an offense when they are used to store drug or fraud transaction data (such as names, dates, and amounts) or to store stolen password lists, credit card or calling card numbers, proprietary corporate information, pornographic image files, or "warez" (pirated commercial software). A computer can also be a tool for committing an offense in its capacity as a communications tool. Many of the crimes falling within this category are simply traditional crimes that are committed online. Online facilities may be used to further a broad range of traditional unlawful activity. Email and chat sessions, for example, can be used to plan or coordinate almost any type of unlawful act, including the communication of threats or extortion demands to victims.

In each of these roles, the process involved in creating, saving, and deleting information and files on a computer often leaves information behind on storage media (i.e., hard drives, floppy disks, CD-ROMs) that can be recovered by a trained investigator. In light of this, a new challenge facing pretrial services and probation officers is the potential need to monitor or examine electronically stored information to determine if a defendant has violated the conditions of release.

According to David N. Adair, Jr., Associate General Counsel at the Administrative Office of the U.S. Courts, monitoring the use of a specific computer or connected device through examination of its hardware or software constitutes a "search." The Criminal Law Committee of the Judicial Conference approved a Model Search and Seizure Policy, which was authorized for distribution by the Judicial Conference in 1993, and districts considering implementing search conditions are strongly encouraged to adopt the policy.

The Model Policy is concerned with the methods and conditions under which Probation Officers may conduct searches. Because pretrial services officers have more limited law enforcement authority than probation officers, the Model Policy does not address Pretrial search issues. However, if "*narrowly tailored to fit the needs of a particular individual*," the Court as a condition of release on a bond may specifically grant search authority.[8] The Model Search Policy rightly takes a narrow view of conducting searches and states a search should only be conducted when: 1) there are no alternatives available and 2) reasonable suspicion exists.

Although the location, nature, and volatility of electronically stored information that officers require to verify compliance or document noncompliance with conditions in these cases would appear to warrant periodic random searches, this is strictly discouraged under the Model Search Policy. The Criminal Law Committee stated this type of search should be conducted only when specifically authorized by a special condition of release.[9] Supervising officers should exhaust traditional verification methods, including examination of the records of online service providers (which may require specific release of information or a court order, depending upon the circumstances), billing and credit card records, as well as service contracts, before resorting to a search. Districts considering recommending the imposition of search conditions should first develop and adopt a search policy.

Once issues related to establishing a search policy are dealt with, consideration has to be shifted to the technical aspects of conducting a search on a computer. If the defendant has been prohibited from possessing a computer or some type of telecommunications device, service, or program, a physical “plain view” search of the home may be the only method necessary to verify compliance. If the court allows the defendant to use a computer or have access to the Internet, it may become necessary to employ more sophisticated monitoring techniques, including a “physical” search of the computer. This step should not be embarked upon lightly, nor should it be initiated without specialized training. If proper precautions are not taken, the data stored on the computer, data disks, or any number of other peripheral devices can be altered, destroyed or rendered inadmissible for court purposes. There is currently no case law spelling out when computer searches by a probation or pretrial services officer are permissible and what the limitations of such searches are.[10]

Depending on the skill level of the defendant, data could be stored in hidden sections of a hard drive, renamed to look like an innocent file type, encrypted, password protected, or may have been deleted. Special tools and skills are required to locate and attempt to retrieve data that has been altered in these ways. In spite of how fast computers operate, conducting a thorough inspection and retrieving documentation of condition violations or new law violations can be a very time-consuming operation, so staff resources must also be a concern.

Consideration must also be given to the level of involvement of automation personnel in the process. There have been instances in several districts where automation staff members have been asked to accompany probation or pretrial services officers to assist with a search or retrieval of information from a computer system. Thorough examination of such a practice may lead to the conclusion that it ought not be allowed to continue. The search of a home, or a computer in a defendant’s home, should be considered a potentially volatile and dangerous undertaking. Automation personnel have neither the training to protect themselves and others in a dangerous situation nor do they enjoy benefits of the hazardous duty designation shared by probation and pretrial services officers. A more prudent approach might involve training officers in the specific skills needed to retrieve an exact copy of the data on a computer and returning it to the automation staff or a trained officer to conduct a thorough forensic examination of the data.

The issue of searching and seizing data from computers also raises concerns about privacy, not only of the defendant, but also of third parties who may reside at the same location and share access to computers. The Electronic Communications Privacy Act (ECPA -18 USC §§ 2510 & 18 USC §§ 2701)[11] impacts information and data that may be housed on a computer system. An examination of the statutes indicates that in dealing strictly with the search of a defendant’s computer, pretrial and probation officers probably do not have to be concerned about exposure to civil or criminal penalties, except when dealing with unopened email. Depending on the physical location of the message (whether it is on the defendant’s computer or a remote server), ECPA provisions may proscribe the viewing of the unopened message.

If the defendant shares the use of a computer with one or more parties, it could be possible to violate the act and be subject to sanctions. Methods to address this issue may include use of written consent forms and posting of a notice on the computer that its contents are subject to inspection. For defendants released on a bond, there is also the possibility of making the persons who share access to the system custodians on the bond, thus giving them a vested interest in ensuring compliance with the conditions.

The impact of technology and the rise in computer-related crimes may cause the field to seek additional guidance regarding computer searches from the Judicial Conference. In the meantime, it appears that the best course of action would be to pair the implementation of a search policy with special conditions of release to allow for random searches limited to address specific behavioral controls such as enforcing a prohibition against possession of pornographic material or use of encryption technology.

Training Issues

A handful of districts in the country have begun to research and use methods to monitor defendants’ computer use and to conduct computer examinations to corroborate compliance problems. Most have entered into this technological quagmire with little or no expertise other than an officer who had a keen interest in technology and a willingness to experiment. Through the efforts of the Federal Judicial Center and the Federal Probation and Pretrial Services Officer’s Association, awareness is being raised and it is being recognized that in order to preserve the integrity of the information we provide to the court, we must become appropriately trained in forensic techniques.

Fortunately, several federally funded agencies have opened the doors to allow probation and pretrial services officers to attend forensics training. Among these is the National White Collar Crime Center (NW3C), the Federal Law Enforcement Training Center (FLETC) and SEARCH, The National Consortium for Justice Information and Statistics. While initially reluctant to provide training to non-traditional law enforcement officers, these organizations have since recognized the efficacy of providing training to our field. This shift was, in part, due to the growing backlog of examinations being experienced by computer forensics labs operated by the Federal Bureau of Investigation, the U.S. Secret Service, and U.S. Customs Service.

These programs offer basic and advanced computer forensic training courses and cover topics from identification of computer hardware to examining and retrieving digital information from hard disks and other digital media. The programs provide an assortment of free tools to assist in the examination process and expose attendees to several commercially available applications designed to streamline the information recovery process. Districts considering adopting a search policy and embarking on monitoring of defendants’ computer use should consider making the training available. Officers who wish to attend one of the basic courses should possess a working knowledge of computers and the MSDOS and Windows operating systems at a minimum. Completion of a basic forensics course is usually a prerequisite for participating in an advanced program. Demand to participate in the programs is high and there are waiting lists to attend. The classes last from one to two weeks and tuition costs range from free to several thousand dollars.

Establishing a Forensics Laboratory

While staff training is being completed, consideration should be given to setting up and equipping a laboratory to facilitate the analysis process. In some cases, attempting to conduct an analysis in the field is not practical, nor is it the safest method to employ. The ideal, according to forensic investigators from the FBI and U.S. Secret Service, is to obtain an exact copy or image of the media to be examined in a secure laboratory setting following the seizure of the suspect computer. In some instances, when seizure is not possible, this image may be obtained in the field and then removed to the laboratory. For probation and pretrial services purposes, seizure may not be the least intrusive method to utilize, but cannot be ruled out if an image cannot be obtained safely or in a timely fashion.

An assortment of hardware and software is necessary to establish a viable lab. The exact configuration depends on a number of factors, including the training level and abilities of the examiner. Access to a number of computer operating systems, including MSDOS, Windows (Version 3x through 2000 and Windows NT), and Linux/Unix is necessary. Laboratory workstations need to be flexible enough to allow the examiner to easily add and remove hardware and be robust enough to perform memory-intensive search and retrieval operations. The lab should be equipped with a variety of external storage devices (i.e., SCSI and IDE CD-ROM and Hard Disk Drives, Iomega Zip and Jazz Drives) or have a budget flexible enough to allow for the purchase of additional devices as may be necessary.

In addition to the laboratory workstations, a portable workstation is recommended to allow for a less intrusive "preview" of a system using software tools to look for specific file types or information. If no violations are evident, it may not be necessary to take further action. The portable unit would facilitate field examinations of a computer system if absolutely necessary, and would allow the examiner to perform analyses at remote locations such as a remote division office. Any portable system should be configured with a variety of storage device options to allow for the retrieval of disk images in as short a time as possible. While smaller and portable, the unit should be able to perform the same software tasks as a laboratory workstation. Some examiners choose to use laptop systems with external storage device options, while others profess that a "luggable" type system that is a scaled-down version of a desktop computer with removable drive bays and an attached LCD monitor is the best option for a portable field workstation.

There are few companies producing forensically sound integrated software to perform an examination on a computer. Unfortunately, the market is still small, so the software tends to be expensive and often requires the examiner to receive additional training to gain a level of proficiency with it. There are a number of sources for "free" applications and utilities that perform some of the tasks that are automated by the integrated applications, but they also carry a steep learning curve and, because they are not integrated, tend to require more time to perform the same functions as the integrated packages. Information disseminated in the training programs sponsored by the NW3C and FLETC as well as discussion with active forensic examiners indicates that the favored procedures are to use an integrated package to perform the analysis on a system and then use the standalone applications to corroborate findings. In addition to the actual forensic software packages, many labs use commercially available programs to recover or "crack" password protection schemes built into popular word processing, spreadsheet, and database applications.

The costs of establishing a functional forensics examination lab are another concern. The Bexar County District Attorney's Office in San Antonio, Texas, recently received a grant to fund the establishment of a computer forensics laboratory. They initially budgeted $16,000 for equipment and $11,000 for software. They purchased three standalone workstations for the laboratory, a "luggable" system to perform field analysis, two portable hard-drive duplicating devices, as well as an assortment of software and remained within their budgetary constraints. These costs are not out of the ordinary for a small laboratory, according to members of the Computer Forensics Information Digest (CFID), an Internet-based discussion group comprised primarily of forensic investigators at the federal, state, and local level. Any budget for the establishment of a lab should also include allowances to purchase new technology, larger form-factor storage devices as they become available, software updates, and ongoing training for the examiners.

The cost of establishing a laboratory, when coupled with the expenses related to staff training, may be prohibitive for many districts. A subgroup of probation and pretrial services officers who were involved with the FJC on the Special Needs Offender program on Cyber Crime formulated a proposal for the establishment of one or more regional laboratories to serve as a resource for forensic analysis and training. With the support of both a Chief Pretrial Services and Chief Probation Officer, the proposal has been submitted to the Federal Corrections and Supervision Division of the Administrative Office of the U.S. Courts and steps are being taken to analyze the proposal.

Conclusion and Recommendations

The explosive growth of the Internet and concomitant advances in technology during the past decade have spawned a new breed of criminal and provided a plethora of tools to aid more traditional criminals in their endeavors. Regrettably for those of us in the criminal justice system, the "bad guys" gained an early advantage. The knowledge vacuum created in our system by their nimble adoption of technology has been recognized and is being addressed as rapidly as possible. Training programs for law enforcement agencies have shifted into high gear in an effort to close the knowledge gap. Unfortunately, the growth in new case filings is currently outdistancing the ability to train investigators and is resulting in growing backlogs of investigations and prosecutions.

Congress has recognized the threat posed by computer crime and is in a mode similar to when they began enacting legislation to deal with the looming menace of "crack" cocaine. New laws are being introduced to address new crimes and enhance penalties on old crimes that are being committed using computer technologies. Commissions have been formed to address the problem within our borders and internationally. Since 1992, the U.S. Department of Justice has asked the U.S. Sentencing Commission to promulgate new guidelines and enhance others to ensure that offenders convicted of high-tech crimes are appropriately sentenced.

Where does this leave the courts? Across the country, U.S. pretrial services and probation officers are reporting increases in number of cases coming to them for investigation and supervision. Since specific computer-crime statistics are not tracked, only anecdotal information can be used to advise the Judicial Conference and the Administrative Office and/or to request guidance and assistance. Just looking at the growing numbers of cases under investigation and pending prosecutions should be enough to warn of an impending crisis. Instead of waiting until another congressionally targeted initiative like the "Weed and Seed" program from the mid-1990s is at our doorstep, or until the knowledge gap among the law enforcement agencies begins narrowing, the courts must take a proactive stance.

This suggests the initiation of a campaign to meet the challenges posed by these technologically savvy defendants. A four-tiered line of attack that incorporates the strategies outlined above includes: 1) the identification or hiring of qualified staff; 2) the development of training programs (both internal and external); 3) the adoption of computer search/seizure policies; and 4) the creation and funding of one or more regional laboratories to conduct forensic examinations.

The foundation for this initiative has already been laid. Resources have been identified and a growing pool of expertise is available within the probation and pretrial services system to tap for assistance. This is the proper time for the Federal Corrections and Supervision Division to take the lead in establishing a program, with assistance from the field, for presentation to the Criminal Law Committee and eventual adoption by the Judicial Conference.

References

1. Children Families and the Internet 2000, a survey of 1,735 parents of children aged 2-17, and 601 children aged 9-17 from the same households. Grunwald Associates, 1793 Escalante Way, Burlingame, CA 94010. (www. grunwald. com)

2. From the Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime Before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Information,Washington, D.C. March 28, 2000. http://www.cybercrime.gov/freeh328.htm.

3. "Issues and Trends: 2000 CSI/FBI Computer Crime and Security Survey," Computer Security Institute. http://www.gocsi.com.

4. Arthur L. Bowker, "The Advent of the Computer Delinquent," FBI Law Enforcement Bulletin, Volume 69, No. 12 (December 2000): 7-11.

5. Internet Integrity and Critical Infrastructure Protection Act of 2000. The bill, introduced by Judiciary Committee Chairman Orrin Hatch of Utah, lost some of its strictest measures in the debate process, as some argued that its original guidelines would over-federalize many minor offenses. For example, the bill originally would have authorized federal prosecution of any juvenile accused of a felony computer crime. As amended, the bill calls for federal prosecution of juveniles only for the most serious offenses.

6. Laura Davis, Marilyn D. McShane, and Frank P. Williams, III, "Controlling Computer Access to Pornography: Special Conditions for Sex Offenders," *Federal Probation* June 1995.

7. Ed Harrison, "Supervising the High-Tech Offender," 1998.

8. Letter from David N. Adair, Jr. Associate General Counsel, to Mr. Joseph P. Brignone, U.S. Probation Officer, Buffalo, NY, dated March 17, 1998.

9. Mark Sherman, "Issues and Tools for Investigation and Supervision," *Special Needs Offenders Bulletin: Introduction to Cyber Crime*, August 2000.

10. David N. Adair, Jr., Associate General Counsel, "Guidance on Searches and Seizures," *News and Views*, Vol. XXVI, No.8 (April 9, 2001).

11. ECPA updated title III, Omnibus Crime Control and Safe Streets Act of 1968. It extends privacy protection to modern technologies and primarily impacts the wiretap statute (18 USC §§ 2510 - http://www4.law.cornell.edu/uscode/18/ch119.html#PC119) and stored communications access statute (18 USC §§ 2701 - http://www4.law.cornell.edu/uscode/18/ch121.html#PC121). It was primarily designed to protect *contents* of electronic mail, voice mail, and remote computing services.