Volume 68 Number 3

Federal PROBATION
a journal of correctional philosophy and practice

An Introduction to the Supervision of the Cybersex Offender

Endnotes

Art Bowker, Computer Crime Specialist, U.S. Probation, Ohio Northern
Michael Gray, U.S. Probation Officer, U.S. Probation, Ohio Northern

ADVANCED TECHNOLOGIES are increasingly becoming a way of life for our society. Computers are found in every home, school, and business, with more and more individuals going "online" every day. Unfortunately, these advanced technologies (computers, scanners, digital cameras, the Internet, etc.) are becoming the tool of choice for the "cybersex offender." Probation and parole officers must become acquainted with how cybersex offenders utilize these new tools in order to manage the risks posed by this offender population.

back to top

Who is the Cybersex Offender?

Cybersex offenders use computers to view, store, produce, send, receive and/or distribute child and other forms of pornography; to communicate, groom, and entice children and others for victimization; and to validate and communicate with other sex offenders. The U.S. Department of Justice 2000 guide, [1] *"Use of Computers in the Sexual Exploitation of Children,"* identifies three general types of cybersex offenders. They are 1) the dabbler; 2) the preferential offender; and 3) the "miscellaneous"offender. Dabblers are described as curious adults with a newly found access to pornography or offenders who are profit-motivated to deal in child pornography. A dabbler could also be the typical adolescent searching for pornography who downloads child pornography. The next group is the preferential offender. This is the sexually indiscriminate individual with a wide variety of deviant sexual interests or a pedophile with a definite preference for children. The last group, the "miscellaneous" offenders, are pranksters or misguided individuals conducting private investigations or exposés who have been found in possession of child pornography.

back to top

Advantages In Using Advanced Technologies

Cybersex offenders find the computer and/or Internet a compelling tool in their deviant behavior for four general reasons. First, Internet access provides the offender with a level of anonymity that is not present in the real world. The offender can communicate with whomever he or she wants with little fear of being readily discovered and/or identified. Offenders communicating online with juveniles can be anyone they want. They can become someone from the opposite sex, another child, more attractive, less overweight, etc. The possibilities are endless. The ability to be anyone they want to be online is a big asset for someone trying to entice a juvenile.

Second, sex offenders using computers can "groom" multiple victims, even simultaneously. Such activity would be much harder in the real world.

Third, the computer greatly enhances the storing, cataloging, and retrieval of offenders' pornography collections. Literally thousands of pornographic images can be stored and concealed on a computer. These images can easily be kept out of sight of family members and inquisitive probation/parole officers, but at the same time be readily available for the offender's viewing and other purposes. This makes the storage of material much easier than if the images were in hard copy form.

Finally, advanced technologies permit anyone to produce pornography. Innocent images can be created and converted to pornography through a process called "morphing." [2] Offenders can even put themselves into pornographic images with a computer. Offenders can also easily take digital pictures of their victims, without having to be concerned about getting the film developed.

back to top

Effects of Cybersex Offenses on the Victim

The effect of cybersex offenses can often be more detrimental for the victim than effects of other offenses. Pornographic images electronically maintained do not deteriorate like hard-copy images. Additionally, they can be distributed easier and faster and have a wider distribution audience than hard-copy images. Once distributed on the Internet, they are harder to retrieve and control. These factors tend to transform electronic pornographic images into media with a longer duration of harm for the victims portrayed than traditional hard copy images.

The Internet also provides a method for the cybersex offender to affect the victim without any physical contact occurring. Consider for a moment incidents where juveniles are exposed to pornography that was forwarded to them by adults. Also, no physical contact occurs when cyber-offenders obtain innocent images of children via the Internet or other sources and then "morph" those images into pornography. Such images may not even be known to the child for some time, until they begin surfacing online.

The nature of the Internet is such that no one country or authority governs its content. Issues of child pornography and exploitation frequently transcend jurisdictional boundaries, causing not only legal problems but also difficulties for victims seeking redress or a remedy.

Additionally, electronic images, just like hard-copy images of child pornography, are used by sex offenders to encourage or entice children to engage in inappropriate sexual conduct. The sending of these electronic images, however, takes on increased importance when they can be so readily transmitted to "future" victims. Finally, the trading of electronic images of child porn between offenders provides a form of reinforcement to these offenders.

back to top

Determining What You Have

Determining what type of cybersex offender you have involves examining the following general areas: 1) files found in the offender's possession; 2) the offender's equipment and Internet

Service Provider(s) (ISP); 3) the offender's online activities; and 4) other activities of the offender. Looking at these areas individually and in conjunction with one another helps assess the offender's commitment to deviance.

Files Found

Knowledge of the files found in the offender's possession is very important. Obviously, sheer quantity reflects the offender's commitment level. Other areas to be aware of are types of files found. Specifically, were they still images, such as those with a file extension of .jpg, .bmp; .gif, etc., or were they moving images, such as those with a file extension of .avi or .mpg? Having a collection of moving images reflects a different aspect of offender behavior than just having still images. Additionally, it takes longer to download moving images than it does to download still images. An individual with a large collection of moving images shows an advanced degree of commitment to getting them because of the time involved in amassing them over the Internet. Finally, moving images take more electronic space to store than still images.

What were file names of the images? Were the names descriptive? This is important because it can counter the cybersex offender's claim not to know that the images were of child porn. Were the pornographic files found in the temporary Internet folders or did the offender save them in specific folders of his choosing? Did the offender's pornography reflect a specific theme and how were the images organized? Was there a particular age group or possible sadistic or masochistic (S & M) images? These issues provide important information on the offender's areas of interest or deviancy. Organization of the images is also significant because it takes active offender participation. It obviously takes a certain level of commitment to organize and sort hundreds or thousands of images.

How many pornographic files were saved on the offender's computer? How many such files did the offender forward to others or did the offender receive from others? This information provides insight into the offender's involvement with the community of deviancy. Additionally, did the offender forward any child porn images to juveniles? Remember, this can be one of the initial online activities to entice children into sexual acts.

In all of the above incidences—i.e., possession, receipt, and distribution—what were the percentages of child porn to adult porn? Specifically, let's suppose an offender has 1,000 pornographic images on his or her computer. Of that 1,000, only 15 were of child porn. This offender shows a different level of commitment from the offender with 1,000 images, of which 900 were of child porn. Likewise, did the offender have a high percentage of violent pornography, such as rape and torture themes?

Finally, how were the images used by the offender? Did he masturbate to them? Did he use them to entice children? Does he claim he has them so that he won't abuse children? Are they used to enhance his "status" with other individuals who collect child porn, i.e, my collection is larger and better, etc.? Did he use them to barter for other forms of pornography (adult, incest, S & M, bestiality, etc.)? Was he involved in selling child pornography?

Equipment and ISP

Offenders' equipment also provides insight into how committed they are to deviancy. Top of the line computers, scanners, digital/ video cameras, etc., may reflect an interest in producing and/or viewing "quality" images. Also, the offender may want large hard drives to store more image files, as they take more space. Better equipment also can provide faster access to images for viewing. Additionally, better equipment can facilitate the production of media containing child pornography to distribute to others.

Beware of what type of ISP offenders have or had. Dial-up services (AOL, Compuserve, MSN, etc.) are slower for downloading image files. Cable and DSL connections provide faster Internet speeds and make it easier to download these files. Again, remember to look at all factors together. For instance, two offenders, both with the same number of moving image files, may

have different levels of commitment if one considers how they obtained the images. Specifically, one offender may have a dial-up service and the other may have obtained the images with a cable service. The first offender would have had to spend more time downloading the images than the second offender because of the slower speed of the dial-up Internet connection.

Online Activities

Information about offenders' online activities is equally important in identifying the type of offender. How many screen names do they have and are any of the names suggestive, implying some deviant interest? For instance, the screen name K9trainer123 may reflect that the offender has an interest in bestiality. Did an offender have a screen profile and what interests did the profile mention? Was the offender's photo on the profile? Was the profile accurate? For instance, did the profile reflect the offender's true age and gender or did it claim that the offender was a child or maybe a member of the opposite sex?

How long has the offender been accessing the Internet: one year, five years, or ten years? How much time did the offender spend online and was the offender frequently online when juveniles were present, such as after school or before 9:00 p.m? How many people communicated with the offender? How many names were in the Buddy List (for chats) or email address book? Were these names of other adults or juveniles? Were the other adults possibly interested in child porn? How many messages, with and without attachments, did the offender send or receive? What were the favorite websites? Was the offender paying for access to porn sites? Did the offender use file-sharing programs such as Kazaa, Bearshare, Napster, etc., to obtain and trade porn?

In cases involving enticement over the Internet, what did the messages/chats reflect? What was the offender discussing? Were there references to S & M, incest, etc. themes? If possible, obtain copies of these messages to include in reports and for the supervision file. The text of such messages can be very useful during treatment when offenders attempt to minimize or rationalize their conduct. Equally important are the items the offender brought to any planned meeting with a juvenile or undercover officer posing as a juvenile. Possession of digital cameras, condoms, sex toys, handcuffs, whips, blindfolds, weapons, drugs (including sexual enhancement drugs), etc. sheds a spotlight on the offender's intentions during and after the encounter. One graphic example is an offender who was arrested in an undercover sting operation to which he brought a shovel, axe, gasoline, and garbage bags to meet someone he thought was a minor.

Other Activities

What were the offenders' real world activities? Have they been employed in jobs involving juveniles? Are they or were they involved in voluntary activities where juveniles are active (Boys Club, YMCA, coach, etc.)? Do they reside near places juveniles frequent or are there juveniles in the home? An offender's history of organizing life around juveniles is an indication that the offender may be strongly drawn to minors.

Does an offender have a history of extensive foreign travel (certain countries are lax in enforcing laws prohibiting sex acts with minors)? Does the prior record include sex offenses with or without computers? Past convictions for such conduct help assess possible future risks.

What kind of educational and work experience do sex offenders have? Are they skilled in computers and/or advanced technologies? Does the record show a prior period of supervision in which monitoring software/hardware was circumvented? This information is important in deciding how best to monitor or manage sex offenders once they are on supervision.

back to top

Conditions to Recommend

Computers can dramatically increase the effects of criminal behavior, and their misuse therefore poses a unique risk to the community. Pedophiles, from the safety of their homes, can anonymously "groom" numerous children simultaneously by computer for later molestations.

Child pornographers can effectively distribute their "collections" to hundreds of other offenders, or even to other children, with the click of a mouse. But while a computer poses a risk, it can also be a legitimate tool for an offender trying to become a productive member of society. Offenders, like others in our community, can use computers to the benefit of all. A blanket prohibition against all access to a computer and/or the Internet during the period of supervision may not always be realistic nor consistent with current case law. The least restrictive yet effective conditions are the most desirable. Probation and parole officers should embrace both traditional and "high tech" tools to manage the risk posed by cybersex offenders, consistent with their agency's directives.

The decision to recommend discretionary computer conditions should be based upon the following criteria: probation/parole law in the particular jurisdiction; the offense of conviction; computer knowledge/skills of the offender; prior criminal conduct involving computers; necessity of the offender to have computer/Internet access; and the availability of a computer or the Internet to the offender. Based upon this evaluation, appropriate computer conditions can be recommended.

As previously indicated, officers should determine what type of cybersex offender they have. Obviously, more restrictive conditions should be considered for offenders who have personally victimized a minor or demonstrated a willingness to do so. For instance, a traveler (offender who travels across state lines to have sex with a minor) poses a different risk than an individual convicted of simple possession of child pornography.

Monitoring software/hardware, coupled with computer search/seizure, serves as the "least intrusive and restrictive" method for controlling the risk that may be posed by most cybersex offenders. Offenders are permitted to use a computer and access the Internet, with the clear understanding that their computer activities are being monitored. The use of high-tech monitoring techniques also allows offenders to remain in households where a computer exists for use by family members. [3] Monitoring limits the requirement to do in-depth computer searches, an endeavor that requires training, equipment, time, and money. Forensic computer searches can be saved for cases 1) in which a tamper to the monitoring operation has occurred; 2) in which the monitoring captures a violation of supervision; or 3) in which there is a new law violation, such as a download of child pornography. [4] Finally, monitoring software/hardware can overcome some of the problems associated with an offender using encryption and/or stenography. Specifically, monitoring can capture what is being hidden and how, as well as capturing passwords used by the offender in the process. To be effective, computer conditions must: 1) establish the offender's access to computers and the Internet; 2) provide a method for controlling or limiting access to what can be monitored; and 3) have a method for monitoring.

There are three general classes of computer conditions for cybersex offenders. All three provide for search and if necessary seizure of any computer found. The first is a total prohibition of access to a computer and the Internet. The second permits access to a computer but not the Internet. The third allows access to a computer and/or the Internet, but access is closely monitored through a combination of high tech and traditional supervision techniques.

With these three classes in mind, prohibitions against computer and/or Internet access should only be recommended for those cybersex offenders who have clearly demonstrated they are unwilling to comply with a less restrictive condition or for offenders who pose such a high risk to the community that no other condition can manage them. The following are the computer conditions used by Ohio Northern, U.S. Probation Office, in sex offender cases, from most restrictive to least restrictive:

Option A: Total Prohibition of Access to a Computer and Internet

1. "You are prohibited from access to any computer, Internet Service Provider, bulletin board system or any other public or private computer network or the service at any location (including employment or education) without prior written approval of the U.S. Probation Office or the Court. Any approval shall be subject to any conditions set by the U.S.

Probation Office or the Court with respect to that approval.

2. You shall submit your person, residence, place of business, computer, and/or vehicle, to a warrantless search conducted and controlled by the United States Probation Office at a reasonable time and in a reasonable manner, based upon reasonable suspicion of contraband or evidence of a violation of a condition of release. Any computer found is subject to seizure and/or search. Failure to submit to this condition may be grounds for revocation. You shall inform any other residents that the premises may be subject to a search pursuant to this condition."

Option B: Computer/Internet Restricted

1. "You are prohibited from 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 conditions set by the U.S. Probation Office or the Court with respect to that approval.

2. "You shall consent to the U.S. Probation Office conducting periodic unannounced examinations of your computer system(s), which may include retrieval and copying of all memory from hardware/software and/or removal of such system(s) for the purpose of conducting a more thorough inspection and will consent to having installed on your computer(s), at your expense, any hardware/software to monitor your computer use or prevent access to particular materials. You hereby consent to periodic inspection of any such installed hardware/software to insure it is functioning properly.

3. "You shall provide the U.S. Probation Office with accurate information about your entire computer system (hardware/software); all passwords used by you; and your Internet Service Provider(s); and will abide by all rules of the Computer Restriction and Monitoring Program." [5]

4. "You shall submit your person, residence place of business, computer, and/or vehicle, to a warrantless search conducted and controlled by the United States Probation Office at a reasonable time and in a reasonable manner, based upon reasonable suspicion of contraband or evidence of a violation of a condition of release. Failure to submit to a search may be grounds for revocation. You shall inform any other residents that the premises and your computer may be subject to a search pursuant to this condition."

Option C: Computer/Internet Access Permitted

1. "You shall consent to the U.S. Probation Office conducting periodic unannounced examinations of your computer system(s), which may include retrieval and copying of all memory from hardware/software and/ or removal of such system(s) for the purpose of conducting a more thorough inspection and will consent to having installed on your computer(s), at your expense, any hardware/software to monitor your computer use or prevent access to particular materials. You hereby consent to periodic inspection of any such installed hardware/software to insure it is functioning properly.

2. "You shall provide the U.S. Probation Office with accurate information about your entire computer system (hardware/software); all passwords used by you; and your Internet Service Provider(s); and will abide by all rules of the Computer Restriction and Monitoring Program."

3. "You shall submit your person, residence, place of business, computer, and/or vehicle, to a warrantless search conducted and controlled by the United States Probation Office at a reasonable time and in a reasonable manner, based upon reasonable suspicion of contraband or evidence of a violation of a condition of release. Failure to submit to a search may be grounds for revocation. You shall inform any other residents that the

premises and your computer may be subject to a search pursuant to this condition."

back to top

Computers and Employment/Education

Offenders will have access to computers at work, at school, and/or public institutions, such as the library. Most institutions have a vested interest in insuring that their systems are not misused and usually have some kind of internal monitoring in place. Traditional techniques of supervision, such as third-party contacts, can ascertain that such procedures are in place. However, an offender employed as a systems administrator or in a similar position creates a unique concern for monitoring. Offenders employed as systems administrators can circumvent all monitoring that may normally be present in the employment setting. In fact, they are frequently the ones in charge of the monitoring of the employer's computer system. Depending upon the circumstances and the risk posed by the cybersex offender, an employment prohibition may be warranted. The following additional condition is suggested in such cases:

"You cannot be employed directly or indirectly where you are systems administrator, computer installer, programmer, or "trouble shooter," for computer equipment or any similar position."

back to top

Traditional Conditions

Traditional conditions for sex offenders should also be utilized. Examples of such conditions are limiting contact with minors, mental health and/or substance abuse treatment, and the use of polygraph testing. The use of polygraph testing is particularly important as an additional method to determine if the offender has, in some manner, overcome the monitoring process.

Limiting/Controlling Access

The first step in limiting or controlling offenders' access to computers and/or the Internet is to establish what access they currently have. In Ohio Northern and many other jurisdictions, this is done with the use of a questionnaire that all offenders with computer conditions are required to initially complete and periodically update. Falsification of these questionnaires can be grounds for not only a violation of supervision but also new criminal charges. Additionally, the veracity of these offender-provided documents is checked through home inspections and contacts with third parties.

Once an offender's computer/Internet access is established, it becomes necessary to decide what computer(s) he or she may continue to access. This process frequently requires not only thought but tact as well. If an offender has computer access at his employment, contact is made to establish what measures are in place to monitor employees' computer access and if necessary to obtain a waiver to install monitoring software on the offender's work computer. Uncooperative employers can create difficulties, which may necessitate directives (with appropriate supervisory authorization) for the offender to seek employment elsewhere. If an offender has several computers at home, it may be necessary to install monitoring software/hardware on all of them or direct the offender to only use certain computers.

Officers installing monitoring software/hardware should also be comfortable opening computer cases to insure that information provided by an offender is accurate. An offender could have two hard drives in a system and attempt to circumvent monitoring by only disclosing one. Visual inspection helps minimize this issue. Once it is decided to install monitoring software/hardware, tamper tape is used to seal the case and pertinent ports, to insure the offender does not later attempt to circumvent monitoring by replacing the hard drive with another one that doesn't have monitoring software installed.

All traditional techniques for supervising offenders remain of value with the cybersex offender. Contacts with third parties can be used to determine if an offender has overcome monitoring

software or used a computer in a manner inconsistent with his or her supervision. Home inspections can establish the existence of a computer system in the home. The examination of bank and credit card statements can be used to determine if online purchases have been made or if the offender has additional Internet access.

Additionally, offenders' initial responses to how frequently they access computers and the Internet can be compared to monitoring reports received to ascertain if there is some drop in usage, which may indicate that the offender is accessing a computer/Internet from somewhere other than the system being monitored.

Some may wonder what would prevent an offender from just going out and getting another computer or going to a friend's house or using some other unmonitored computer. The answer is nothing–just as there is nothing but fear of discovery to stop an offender from using drugs or obtaining a gun. However, once non-compliance is discovered, probation/parole officers have demonstrated an attempt to work with the offender while he has demonstrated a lack of willingness to comply. In such cases, more restrictive measures, including prison, may clearly be justified.

back to top

Monitoring Methods

As we have noted, procedures to monitor an offender's computer use include traditional methods, such as home visits and third-party contacts, installation of monitoring software/hardware, and search/seizure.

Traditional methods are well established practices in most correctional agencies. Their usefulness is not diminished with the onslaught of technology. However, officers need to be aware of what to look for during home inspections and what to ask during third-party contacts. Offenders are frequently finding novel uses for new technology and officers must keep up. For instance, when the mini-USB storage devices initially appeared, it did not take long for cybersex offenders to start using them to store and trade child pornography. Therefore, officers must supplement their skills in traditional methods with a healthy dose of technical knowledge.

Software/Hardware

Currently, there is no monitoring software or hardware developed specifically for use by probation/parole officers. However, several vendors provide "off the shelf" products at a reasonable price that can be used by probation/parole officers to supervise the cyber-offender. Two different vendors provide products used by many correctional agencies. Both of these vendors have products that record a computer user's activity, i.e., applications running; screen shots; and key strokes. Both also provide for the periodic, remote forwarding of activity reports. Additionally, both vendors can forward "hot" reports, when key words are typed or detected on a web page. Both vendors have products that provide for some degree of concealment, which facilitates their use against knowledgeable offenders. Finally, both vendors have products that can be installed by officers without extensive computer expertise.

Another option being spearheaded by another company is a service providing realtime monitoring of an offender's computer for the cost of the installation software plus a monthly service fee. Software installed on the offender's computer directs all Internet activity to first go through this company, which records the activity and provides the supervising agency with access to those records. One additional benefit of this service is that officers can remotely limit access to certain sites and applications or prohibit all Internet access if the need arises.

Unfortunately, some operating systems preclude the use of monitoring software or the above service. In some cases hardware devices such as keystroke loggers can overcome this issue. Hardware devices can also be an additional tool, used in conjunction with monitoring software, for particularly "savvy" offenders who may be able to compromise or hack software. Such devices are self-contained and record all keystrokes typed, regardless of whether the system is

even on. These devices can contain up to a year's worth of keystrokes at a time. One has to download the data on site and review all keystrokes for problems areas, which can be a daunting task. Such devices, secured with tamper tape, do provide an additional hurdle for sophisticated offenders to overcome.

back to top

Search/Seizures

Computer searches/seizures should only be conducted by trained personnel. Forensic methods ensure that evidence found can be used in violation proceedings as well as in additional new criminal charges. Initially, at the installation of monitoring software/hardware, it is appropriate to conduct a limited search to ascertain whether the system is "clean" or if any problem software is installed, such as anti-monitoring programs, file sharing programs, etc. Subsequent searches may require more intrusive methods, such as the recovery of deleted files, searching slap space and page and swap files, etc.

Unfortunately, probation/parole agencies are limited in their ability to secure funding for equipment and training. Additionally, probation/parole agencies may not always have the initial technical expertise to determine the appropriate equipment. Some vendors will attempt to provide software that is not forensic-based, noting that probation/parole officers need not worry about law enforcement standards. Often, these programs start up using the offender's own operating system. This should be avoided. Evidence found during a probation/parole search can lead to new criminal charges and shortcuts should not be taken because of the lesser standard of proof required in violation proceedings. Additionally, inappropriate handling of evidence by probation/parole officers may compromise the discovery of other individuals involved in the child sex offenses. For instance, a computer belonging to an offender may have information about people with whom the offender is trading child pornography.

The first step for probation/parole officers is to obtain basic computer forensic training to understand the proper methods for searching and seizing computers. Probation/parole agencies should also initially focus on software/hardware that allows their personnel to conduct on-site searches in a forensic environment, i.e., without changing the data on the offender's computer. Some software programs prevent any writes to an offender's computer systems. Additionally, hardware write blockers can be used to examine computers without making changes to the offender's system. Conducting initial searches in a forensic environment will allow probation/parole officers to "hand over" cases to law enforcement for a complete forensic search and possible new criminal charges.

If feasible, probation/parole agencies should obtain additional software/hardware and training that will allow an offender's computer to be completely processed in a forensic manner, from data acquisition through examination.

back to top

Conclusion

Probation and parole agencies are seeing increases in the number of sex offenders on their caseloads. Many of these offenders are extremely high risk, and access to a computer and the Internet heightens that risk to the community. Like law enforcement, community corrections officers must learn to properly understand and investigate cybersex offenses. The use of monitoring software/hardware and the ability to conduct computer searches and seizures are skills that probation and parole officers must add to their correctional tool kits to supervise sex offenders and protect the community.

back to top

Endnotes