Even before the Internet, pedophiles used computers and modems to communicate, create networks, exchange information on victims and otherwise further their aims. In the 1980s, police broke up several networks of child molesters who used computers to pinpoint potential victims and to coordinate their efforts.

Today, the situation is far worse because of the spread of computers and the popularity of the Internet, which provides worldwide access to anyone with a modem. In nations with traditions of freedom, it is very difficult to prohibit communications that aid pedophiles. Generally, there must be a connection to a specific crime.

U.S. Customs used to seize many pornographic books and magazines entering the country, but this has dwindled because there is no longer much need to send photographic prints through the mail or via commercial parcel services. The Internet enables sending pornography literally with the speed of light through a medium that bypasses ports of entry.

There are many obstacles to prosecution. Advocating a particular sexual practice is not the same as conspiring to commit illegal acts, and this loophole is very convenient for many groups that operate on the borderline. Another problem is jurisdiction, made more difficult and more intractable by the truly worldwide nature of the Internet.

A little-stated fact is that the reason do-it-yourself photographic media, such as Polaroid cameras, camcorders and digital cameras, have sold so well is because they allow discreet, in-the-home photo and movie production. Back when photographs had to go to commercial processors, there was a greater risk in producing pornography. Now, any person with a camcorder or digital camera can produce his own pornography, and even kiddie porn, with much greater safety than ever before.

Images from camcorders, and especially digital cameras, are very suitable for transmission on the Internet. Most digital cameras come with software and connectors to allow uploading into a computer as part of the package. This is why there is a tremendous number of pornographic web sites on the Internet.

By themselves, because of their sheer number, web sites pose a challenge for the investigator. It's a major task to screen all of them to determine which show promise as leads to pedophiles. Physical concealment is one technique. Technologically advanced methods such as encryption is another. Text and photographs can be encrypted so that they are totally unrecognizable except to one that knows what they are and who has the key.

Officers serving search warrants against suspected computer pedophiles should be aware that many of these people are technically sophisticated, and may "booby-trap" their computers to destroy evidence. With modern computer programs, it isn't difficult to generate a "macro" that will erase the entire hard drive with the press of a single key.

Law Enforcement Investigates Abuse

By Tony Lesce
key, while officers are unaware that the evidence is vanishing in front of their eyes.

Likewise, voice recognition programs enable users to execute functions without touching the computer, based on a word or phrase unlikely to be uttered in normal situations. Saying a word such as "arrest" or "I surrender" can trigger a wiping function that will make the hard drive blank within minutes. Several disk-wiping programs are offered by reputable manufacturers to enhance computer security for legitimate users. These remove files from disks and repeatedly over-write them with alternating "1" and "0" symbols to make them absolutely unrecoverable.

One technique that was successful was cutting off power to the computer, either by disconnecting the power cord or flipping the installation’s circuit breaker, before beginning the raid. Interrupting the power no longer works because many computer users today have an Uninterruptable Power Source (UPS) between the wall plug and the computer. This battery back up cuts in when the circuit senses a drop or interruption in power. Its purpose is to prevent losing valuable material in a computer “crash.”

The UPS provides a few minutes’ power, enough for the user to close down his programs and save his material. The criminal also benefits, because the UPS provides enough power to run an erase program.

Another valuable point to note is that a computer must be
"on" to initiate any self-destruct program. One way of exploiting this fact is to serve a search warrant when the subject is not at home, or when there's no guarantee, because many Internet users, legitimate as well as criminal, use their computers during this period because Internet traffic is much less during early morning hours.

**Law Enforcement Agencies**

Local agencies, the first resource for victims and parents of victims, are seldom prepared for this problem. Some larger agencies have special "Crimes Against Children" units that enforce laws against pedophilia. The FBI follows up on federal reports relating to sexual abuse of children, "kiddie porn," and others. Laws such as Racketeering Influenced and Corrupt Organizations (RICO) also include prosecutions of child molesting conspiracies. Field Offices have Special Agents designated as Crimes against Children (CAC) Coordinators.

The FBI has an "Innocent Images" investigation directed at Internet pedophiles. This came about during an investigation in 1993 in conjunction with Prince George's County, Maryland. Two suspects had sexually exploited boys during a 25-year period, and examination of their methods showed that this problem extended far beyond this specific case. It became clear that offenders were using Internet chat rooms to make contact with others, and that children who participated in chat room discussions had no way of knowing the ages or backgrounds of other participants. Similar to chat rooms are "forums," most of which are devoted to legitimate discussions of politics, parenting, hobbies, etc., but some of which concentrate on sexual topics. A novice can be quite surprised at the variety of sexual topics under discussion.

There are also "newsgroups," which do not deal in news, but opinions. Some newsgroup providers make the nature of their topics clear by their names, such as "alt.boys.sex" "alt.pedophilia" "alt.sex.children" "alt.binaries.boys" etc. Newsgroups, like forums, accept "posts," which are statements by readers that may be in the nature of opinions, personal ads, want ads and other offers to make contact. Many are pornographic stories, some of which involve minors and some of which may reflect the authors' real-life experiences. Themes can be heterosexual or homosexual, and contain sado-masochistic and other forms of offbeat sex. All contain disclaimers stating that the characters and incidents are entirely imaginary.

Pedophile organizations such as the North American Man-Boy Love Association (NAMBLA), based in Manhattan, have web sites devoted to justifying sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles. Some post bulletins exposing sexual contacts with minors and exchanging information among pedophiles.
do not act upon their impulses. It's hard to separate these in person, but when all that is visible is an electronic persona on a forum, it becomes impossible. Therefore many leads will evaporate because the subject does nothing overt or illegal.

Investigations require close coordination. One successful international effort in 1998 was worked through Interpol. A tip from U.S. Customs led to Sussex, England, where local police targeted a ring that had many international Internet connections. In the end, police agencies as far apart as Italy, Australia and the United States raided pedophiles and seized their materials, which included over 100,000 pornographic photographs of children.

Types of Investigations

An investigation can begin with a complaint by a victim or parent that a pedophile on the Internet has made contact with his intended victim. Having an officer take the role of the intended victim and lure the pedophile into attempting contact in person can lead to a prosecution.

Another "sting," is officers (usually U.S. Customs and U.S. Postal Inspectors) place advertisements on the Internet offering kiddie porn for sale. Those who order it are subject to arrest if they accept delivery. The crucial point is staking out a post office box or a mail drop, which customers often provide as mailing addresses. Apprehending the suspect with the contraband in his hands is often final.

Officers must be alert to opportunities that comes infrequently, but which can place a wealth of evidence and leads into their hands. One such is when a child molester is arrested by other means, such as being caught flagrant delicto, or as a result of a direct complaint by a victim who can identify him. One New Mexico man made contact with a 13-year-old Tulsa, Oklahoma girl, traveled to Tulsa, where her mother and police caught them at a local motel.

Victim complaints, however, are not very common. One reason is that most victims were seduced, not forced, and are not aware that something bad was done to them. Another is because many child victims respect the pedophile's wish to "keep the secret between us."

Serving a broadly worded search warrant can result in the confiscation of many types of materials. Some, such as clean or soiled children's underwear, may be relevant only to the immediate investigation. Other materials can be useful for further investigations. These include photographs, lists of names, addresses and telephone numbers of other pedophiles, (some belong to clubs) computer disks with similar material on them, and other media.

Photographs serve not only as evidence but also leads, which is why there should be a determined attempt to identify the children in them, even if fully dressed. This isn't as difficult as it might appear because some pedophiles note the child's name, physical characteristics and even descriptions of sex acts on the backs of their photographs.

Another point to watch is that molesters often exchange photographs of their victims. Photographs found while searching one suspect's premises can lead to other molesters. Of course, this
doesn’t apply to commercially produced child porn.

Stories can also serve as leads, if not evidence, because some pedophiles write their accounts of sexual contacts with minors, disguising it as fiction. However, if the story is sufficiently detailed, it can provide leads to places, times and persons. Correspondence with others of similar interests is common, and investigators should carefully scrutinize all letters and envelopes for content.

Other items to seek are receipts for safe deposit box fees and/or storage facilities fees, because these are often repositories for other incriminating material. Besides correspondence files on a computer disk, paper address books can provide the names of friends and acquaintances. A listing in a suspect’s address book isn’t sufficient cause for a search warrant for another individual, but correlating a name with those on other lists can be productive.

The Outlook

Pedophiles have always been ahead of the power curve, and law enforcement has trailed, sometimes far behind, in apprehending them. The Internet is merely the latest area in which pedophiles have captured a huge lead because of their networking and technical expertise. However, the keys to improving law enforcement performance are both technical and organizational.

Officers can become more proficient at working the Internet for leads, and exploiting leads taken in local investigations. Organizationally, police agencies are learning to work together better, abandoning the territoriality that has plagued law enforcement for generations. L&O

Resources:
National Center For Missing and Exploited Children.
U.S. Customs Service
U.S. Postal Inspection Service
Pedowatch. http://pedowatch.org/ This private organization offers information and search engines to trace pedophiles on the net.

Tony Lesce is a free lance writer based in Albuquerque, NM, and a frequent contributor to LAW and ORDER.