By enabling human interaction without the constraints of physical barriers and with the perception of anonymity, the Internet has become the ideal instrument for individuals who wish to intimidate, threaten, and harass others. A stalker can use the Internet to send alarming messages anywhere, within a matter of moments, under the guise of a fictitious screen name or pseudonym. Understanding how offenders use the Internet to stalk victims in cyberspace can provide law enforcement officers with solutions when they encounter impediments investigating these types of cases.

DEFINITION OF CYBERSTALKING

As the Internet becomes the communication device of choice for millions of people worldwide, news headlines, such as “Killer Keeps Web Pages on Victim, Stalks Her Through Internet” and “Penn Opens Hate E-mail Inquiry,” have begun to appear more frequently. These headlines depict stories of criminal intimidation, harassment, fear, and suggestive violence where individuals use the Internet as a tool to stalk another person. The term cyberstalking has emerged to describe the use of such technology to harass or stalk. Cyberstalking is defined as the repeated use of the Internet, e-mail, or related digital electronic communication devices to annoy, alarm, or threaten a specific individual or group of individuals.

All 50 states and the federal government have enacted statutes aimed at protecting the victims of stalking. Many of these statutes have existed for a long time, while others have originated recently. Some of the older statutes were broad enough to cover any type of stalking behavior, including cyberstalking; others had to be amended to do so. In some jurisdictions, new laws specifically addressing the problem of cyberstalking have been enacted. In adapting general stalking and harassment statutes to cover instances of cyberstalking, legislators have expanded the means by which offenders commit this crime to include electronic communication devices.

Several states currently include specific protections against threatening electronically transmitted communications in their stalking or harassment statutes. Additionally, Title 18, Section 875, U.S. Code, criminalizes threatening messages transmitted electronically in interstate or foreign commerce. The use of federal legislation to prosecute cases of cyberstalking, however, is limited, by law, to
instances where the harassing messages are transmitted across state lines or outside the United States. Despite the existence of Title 18, Section 875, the federal government historically has limited its involvement in prosecuting cases related to electronically transmitted threatening messages to cases involving special circumstances, such as threats made against the president of the United States. As with stalking that does not involve the Internet, local authorities investigate and prosecute most cyberstalking cases in either the jurisdiction where the victim resides or in the jurisdiction where the messages originated.

With the rapid pace of technological advancement that exists in today’s society, legislation should take an evolutionary approach toward defining electronic communication devices and systems of transmission. Legislation that limits electronic devices and transmission systems to specific technologies, such as telephones and land-based wires, risk becoming antiquated with the emergence of new technologies, such as computers and wireless transmission systems.

THE STUDY

Background

Anticipating the significant role computers would play in the commission of crimes in the future, the New York City Police Department (NYPD) developed the Computer Investigation & Technology Unit (CITU) in 1995. CITU investigates cases where offenders use a computer or the Internet as an instrument to commit a crime or where a computer represents the target of a crime or constitutes a source of evidence relating to a crime. The unit also performs outreach services to business and community groups to educate people on computer ethics, safe Internet practices, and data security issues related to the most current practices of computer hackers. Additionally, CITU provides training and technical assistance to local, state, and federal law enforcement and prosecutorial agencies.

Methodology

The authors used official police records from NYPD’s CITU to capture data on the extent and nature of cyberstalking for this study. Specifically, the data for this study were drawn from information contained within standardized forms filed by the complainant at the time of the initial complaint and standardized investigative forms that detail the progress of the investigation from beginning to end. Data were gathered using all closed cases of aggravated harassment investigated by NYPD from January 1996 through August 2000 in which criminals used a computer or the Internet as the instrument of the offense. In addition to the date of the offense, descriptive information was gathered on the victim, the offender, the outcome of the case, the method used to harass, and whether the victim and suspect resided in the same jurisdiction.

Extent of the Problem

When compared to other cybercrimes, cyberstalking has been the most prevalent crime...
reported to and investigated by CITU since the unit’s inception. During the 56-month period from January 1996 through August 2000, 42.8 percent of the cases investigated by CITU involved aggravated harassment by means of a computer or the Internet. Additional CITU investigations during this period involved grand larceny, computer and network trespassing, forgery, petty larceny, criminal impersonation, child pornography, crimes against children, and schemes to defraud. Understanding the distribution of cybercrimes is essential to allocating a computer crime unit’s resources in a cost-efficient manner. Training that provides investigators with the technical knowledge and procedural experience needed to successfully investigate cyberstalking should be a priority for a computer crime unit. Agencies should note that the technical training needed to successfully investigate cases of cyberstalking is not entirely crime specific and will prove useful when investigating other types of computer-related crime.

An examination of case outcomes revealed that 192 of the 201 cyberstalking cases investigated by CITU were closed during the 56-month period of this study. Approximately 40 percent of the cases were closed with an arrest, and almost 11 percent of the cases failed to produce evidence that a crime was committed. CITU closed the remaining cases after finding evidence to support the victim’s complaint due to a jurisdictional issue, an uncooperative complainant, a case transfer, or exhausting all investigative leads without positively identifying a specific offender.

The Offender

Offender characteristics were examined using the 134 closed cases where a suspect was arrested or where evidence to support an arrest existed but a suspect was not arrested because of an uncooperative complainant or a jurisdictional issue. The results revealed that males (approximately 80 percent of the cases) were more likely than females to commit aggravated harassment using a computer or the Internet. Approximately 74 percent of the offenders were white, 13 percent Asian, 8 percent Hispanic, and 5 percent black. The average age of the offender was 24, with the oldest offender being 53 years old and the youngest being 10 years old. Approximately 26 percent of offenders were juveniles, according to New York State law, or under the age of 16.

The Victim

Victim characteristics were examined using the 171 closed cases where investigators determined that a threatening or alarming message was transmitted using a computer or the Internet (excluding cases with unfounded outcomes). Females, the most likely recipients, were victimized in about 52 percent of the cases, whereas males were the victims of aggravatated harassment in approximately 35 percent. Educational institutions represented the next most likely target with 8 percent. Offenders chose private corporations in almost 5 percent of the cases. Public-sector agencies were targeted in about 1 percent of the cases.

Approximately 85 percent of victims were white, 6 percent Asian, 5 percent black, and 4 percent Hispanic. The average age of the victims was 32, with the youngest victim being 10 years old and the oldest being 62 years of age.

Technological Methods

In 92 percent of the cases, offenders used only one method to stalk their victims. E-mail was used most often. Offenders used e-mail to harass their victims in approximately 79 percent of the cases. The second method most often used by offenders was the instant messenger. Offenders used instant messengers to harass their victims in about 13 percent of the cases. Chat rooms were used in approximately 8 percent of the cases, while message boards and Web sites were used respectively in 4 percent and 2 percent of the cases. Last, offenders employed newsgroups and false user profiles in approximately 1 percent of the cases.
Cyberstalking Methods

Cyberstalkers have employed various methods of Internet communication to harass their victims. Although not exhaustive, the following list describes some of the methods that cyberstalkers may use:

- **E-mail**: A method of communication that allows an individual to transfer text, picture, video, and audio files to another person’s electronic mailbox. In using e-mail to harass, the cyberstalker creates a text-based, graphic-based, or audio-based message of a threatening, alarming, or otherwise harassing nature and sends it to the e-mail account of the intended victim.

- **Newsgroups**: A method of communication that amounts to an ongoing discussion about a particular topic. Internet users contribute to the ongoing discussion by posting their opinions, comments, or related experiences about a particular subject. These postings are linked together and can be retrieved by querying a database of newsgroup topics. Cyberstalkers can use these forums to post threatening or defamatory statements directed at a specific individual or group of individuals. In *New York v. Munn* (688 N.Y. S.2d 384; 1999), the court found the defendant guilty of aggravated harassment for posting a message to an Internet newsgroup that instructed people to kill police officers from the NYPD.

- **Message boards/guest books**: A method of communication similar to a newsgroup in that its contents amount to comments about a particular topic. Internet sites often have guest books where visitors can enter their names and make comments about the site. The visitor’s name and comments are subsequently available to be viewed by others visiting the Web site. A person who wants to threaten or harass the owner of a Web page easily can leave alarming messages in a guest book.

- **Internet sites**: A method of communication that involves posting information to a unique uniform resource locator (URL). Internet users later can retrieve this information by directing their Web browser to the corresponding URL. An Internet site becomes the method of harassment when a cyberstalker posts information on a Web page about an individual that causes them to become alarmed or frightened. For example, a cyberstalker could create an Internet site that advertises sexual services for hire and includes the victim’s picture, phone number, and address. Subsequently, the victim is bombarded with telephone calls or personal visits from individuals inquiring about the advertised sexual services.

- **Chat rooms**: A method of communication that enables real-time text, audio, and video-based group interaction. Chat rooms, or chat channels, usually are organized around specific topics of conversation. Topics include, but are not limited to, such issues as politics, religion, relationships, and sex. When communicating in a chat room, a participant’s messages are broadcast to everyone signed into the particular chat room. Several types of chat services have emerged since the development of the Internet. Chat services can be public or private. Public chat services are open to everyone with access to the Internet. For example, Internet relay chat (IRC) and I seek you (ICQ) chat are open to all Internet users. Both IRC and ICQ chat rooms have hundreds of chat channels that cover a diverse range of subjects and enable the transfer of files between active participants. Unlike public chat services, private services limit access to their chat channels and are hosted by specific on-line service providers. Chat rooms provide cyberstalkers with different options to harass their victims. A stalker can send alarming messages directly to the victim while conversing in a chat room. The message is delivered to the intended victim, as well as to all those users who currently are logged into the chat room. In addition, the cyberstalker can pose as the victim in a chat room and provide personal information to participants, thereby resulting in the intended victim being directly contacted in person, by e-mail, or by phone.

- **Third-party instant messengers**: A method of communication that enables real-time text, audio, and video-based interaction between two individuals over the Internet or a computer network. Users program their instant messenger software to notify them when designated individuals log on to the network. With instant messaging software, users have the ability to engage in real-time dialogue with a designated person as long as both parties are connected to the network. Stalkers with prior knowledge of a victim’s screen name can use an instant messenger to send harassing messages in real time when both parties are logged onto the Internet.

- **Commercial service user profiles**: A method of communication that involves posting descriptive information about oneself to the membership directory of a commercial Internet service. Service subscribers can query this directory so that they may find other members who share similar hobbies, interests, or backgrounds. People who want to harass others may establish a false user profile that will direct unwanted communication toward their victim in the form of repeated telephone calls, e-mails, or in-person contact.
Knowing the type of Internet technology used most often by cyberstalkers can prove beneficial to law enforcement administrators who must decide how to allocate the training budget for computer crime investigators. Because e-mail constitutes the method most often used by cyberstalkers, unit administrators should prioritize technical training that provides investigators with the knowledge needed to perform e-mail-related forensics.

**ISSUES FACING LAW ENFORCEMENT AND POTENTIAL SOLUTIONS**

Technical features of the Internet and procedural issues with the law present problems for criminal justice agencies when investigating and prosecuting cyberstalking cases. These problems, however, are not crime specific and generally occur when agencies investigate and prosecute cases involving any type of computer crime.

**Jurisdiction**

The global reach of the Internet and the instantaneous nature of computer-mediated communication present law enforcement with jurisdictional issues that could negatively impact the investigation and the subsequent prosecution of computer crimes. With the Internet, stalkers no longer need physical proximity to have contact with their victims. They just as easily can harass a person in another state or country as they can a person who lives in close proximity.

The majority of CITU’s aggravated harassment cases involved investigations where both the offender and victim resided within the jurisdiction of the NYPD. In approximately 72 percent of the cases, the offender and the victim resided within the five boroughs of New York City. In comparison, 26 percent of the cases involved either an offender or a victim who resided outside the jurisdiction of the NYPD but within the United States, while 2 percent of the cases involved an offender from a foreign country.

An offender residing outside the jurisdiction of the investigating agency can negatively impact the outcome of a case. In New York City, the District Attorney’s Office is less inclined to prosecute aggravated harassment cases if the arrest of the suspect requires extradition from another jurisdiction. Such policies have prevented the apprehension of offenders by the NYPD in cases where investigations by CITU have produced evidence supporting their arrests. In 20 aggravated harassment cases investigated by CITU, the NYPD did not arrest the suspects, despite supporting evidence, because their arrests would require extradition from another jurisdiction. In these cases, the NYPD made referrals to the police departments that had jurisdiction over the offenders.

Differences in statutory definitions of stalking across states may complicate the investigation and prosecution processes when offenders reside outside the jurisdiction of the investigating agency. Jurisdictions that do not recognize Internet communication as a viable method to stalk or harass may deny or ignore the extradition request, search warrant, or subpoena of a jurisdiction where

---

**Resources**

- U.S. Department of Justice Cybercrime Web Site: [http://www.cybercrime.gov](http://www.cybercrime.gov)
such methods do constitute a criminal offense.

To minimize the negative impact jurisdictional issues have on the successful investigation and prosecution of cyberstalking cases, computer crime investigation units should develop working relationships with their counterparts in other jurisdictions. Such relationships can prove essential to securing the arrest of out-of-state or foreign offenders in their home jurisdictions when the victim’s jurisdiction will not arrest if extradition is required. In addition, cross-jurisdictional relationships between computer crime investigation units can help secure the execution of out-of-state subpoenas and search warrants and facilitate relationships with out-of-state Internet service providers, computer manufacturers, and software developers. Over the past decade, various professional organizations have formed for those involved with the investigation of computer-related crimes. Participation in these organizations can provide law enforcement with invaluable links to out-of-state resources.

Because of the ease with which cyberstalkers may attack across jurisdictional lines, legislatures should carefully define the venue of the offense. In cases where threatening communication originates from another state or country and the statute of the investigating jurisdiction defines the venue of the offense in terms of where the communication originated, the criminal justice community will not be able to properly serve the victim. When creating legislation to combat cyberstalking or when revising existing stalking legislation to include Internet communication, states should define the venue of the offense in a manner that includes both the place where the communication was received and the place where the communication originated.

"...administrators should prioritize technical training that provides investigators with the knowledge needed to perform e-mail-related forensics."

Account and User Information

The unwillingness of some Internet service providers to readily grant law enforcement access to subscriber records further complicates the investigation of a cyberstalking case. Not all Internet service providers agree on what constitutes subscriber records, which are obtainable by subpoena, as opposed to transactional records, which require a search warrant. When compared to obtaining telephone records from a telephone company, obtaining a suspect’s Internet account information from a service provider can prove far more complicated and involve an increase in the amount of paperwork and time an investigator spends on a case.

Out-of-date and missing account, subscriber, or user information also presents problems to law enforcement agencies when investigating cases of cyberstalking. Without toll records or transactional data, investigators can have a difficult time establishing an electronic link between the suspect and the victim. The financial and human costs associated with gathering and maintaining account information decreases the possibility that Internet service providers will voluntarily collect and maintain such data for a useful period of time. Missing toll records, transactional data, user information, or account content resulted in a negative case clearance in approximately 18 percent of the cyberstalking cases investigated by CITU. In these cases, the content of the communication contained a threatening message, but no arrest occurred because detectives could not gain access to the electronic evidence to legally support apprehending a specific individual. To ensure that account, subscriber, and user information are collected and saved long enough to help law enforcement, legislation that regulates Internet service providers should include data collection requirements.

Anonymizing Tools

The continued development and increased availability of anonymizing Internet tools (i.e., devices that ensure a person’s anonymity when using the Internet) can complicate the investigation of cyberstalking cases. Anonymous
remailers allow individuals to send electronic mail without transmitting any information that would enable others to determine the identity of the author. Remailers strip identifying information from the e-mail header and erase any transactional data from servers that would enable law enforcement to trace the message back to the author. Consequently, cyberstalkers who use an anonymous remailer as the sole means to send threatening or harassing e-mail messages will remain virtually undetectable to the victim and law enforcement. The danger raised by the use of anonymous remailers, as depicted by CITU’s caseload, does not stem from the frequency in which these tools are used, but from the effect these tools have on the investigative process. Anonymous remailers were used in only 4, or 2.1 percent, of the 192 cyberstalking cases investigated by CITU. Investigators, however, could not trace the harassing e-mail messages sent through the anonymous remailers back to their authors in all four cases where these tools were used.

Anonymous Web-browsing services also offer cyberstalkers the opportunity to harass or threaten victims while remaining virtually untraceable to law enforcement. Some companies provide users with the ability to surf the Internet, participate in public chat channels, send instant messages, and post messages to newsgroups without transmitting any identifying information. The exclusive use of such services to send harassing messages would prevent investigators from establishing an electronic link between the victim and the offender. An examination of CITU’s cyberstalking caseload found no instances where offenders used anonymous Web-browsing services to stalk their victims.

The widespread availability of anonymizing tools can increase the amount of cyberstalking and Internet deviance in general. Theoretically, deviance will result from the use of anonymizing tools because people will feel less restrained when not faced with the fear of detection by their victim or the police. The absence of a legally binding international body to regulate the Internet leaves little hope that the deployment of anonymizing tools will be stopped. Even if a country did succeed in banning the distribution of anonymizing tools, the global reach of the Internet would enable people to seek out such tools in countries that allow their use. Consequently, citizens must learn to survive on an Internet where people can act without accountability. In the absence of a regulatory solution to safeguard Internet users against those who employ anonymizing tools to harass, Internet service providers and related software companies should seek a technological solution aimed at blocking unwanted anonymous communication.

CONCLUSION

Because the Internet allows human interaction without physical barriers and with the perception of anonymity, it has become the ideal instrument for individuals who wish to intimidate, threaten, or harass. Federal and state legislation have emerged to criminalize such behavior. Legislatures aiming to criminalize cyberstalking should
take an evolutionary approach toward defining the means of communication covered by the law to ensure protection against harassing communications sent using newly developed technologies.

An examination of all computer crimes investigated by the New York City Police Department from January 1996 through August 2000 found cyberstalking to be the most prevalent computer crime investigated by the department. Thus, police personnel administering computer crime units should prioritize staffing and training initiatives that properly equip their units to deal with the cyberstalking problem. Additionally, because cyberstalkers use e-mail as the communication method of choice, computer crime unit administrators should prioritize technical training that provides investigators with the knowledge needed to perform e-mail-related forensics.

Out-of-date and missing account, subscriber, and user information, as well as anonymizing tools, presented problems for law enforcement during cyberstalking investigations. Working relationships between computer crime units in all agencies can minimize the negative effects that jurisdictional issues have on the investigation and prosecutorial processes. These relationships can help facilitate the execution of out-of-state subpoenas and search warrants and provide law enforcement with an open door to out-of-state Internet service providers.

Out-of-date and missing account, subscriber, and user information also have prevented law enforcement from establishing an electronic link between the suspect and the victim. To offset this negative effect, legislative action should establish data collection standards for Internet service providers that meet the needs of computer crime investigators.

```
All 50 states and the federal government have enacted statutes aimed at protecting the victims of stalking.
```

Finally, the infrequent use of anonymous remailers by cyberstalkers should not pull attention from the negative effect that these tools can have on the law enforcement process. The increased availability and continued development of anonymizing Internet tools that are easier to use than previous versions likely will increase the use of these options by criminals. When used, anonymous remailers successfully prevented law enforcement from tracing e-mail messages back to the offender. A technological solution aimed at blocking anonymous communication will offset the threat to users posed by anonymous remailers. ✷

Endnotes


3 American Prosecutors Research Institute, The Status of Cyberstalking in the Context of Violence Against Women (Arlington, VA: American Prosecutors Research Institute, 1999). For instance, section 240.30 of the New York State Penal Law finds a person guilty of aggravated harassment if the individual purposely intends to harass, annoy, threaten, or alarm another person by means of mechanical, electronic, or written communication. Additionally, New York revised its antistalking statutes in December 1999 to cover electronic communication, such as e-mail, that is likely to cause fear or harm. In defining the actions that constitute stalking, section 646.9 of the California State Penal Code includes verbal, written, or electronic communications that are intended to place individuals in reasonable fear for their safety. In defining electronic communications, California has relied upon the definition used in the U.S. Code for regulating behavior related to communication devices. Specifically, the term electronic communication means “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system.” According to the California State Penal Code, the devices used to transmit electronic communications include, but are not limited to, telephones, cellular phones, computers, video recorders, fax machines, and pagers.

4 New York Penal Law § 240.30

5 As defined by New York Penal Law § 240.30.


7 The legal requirements for obtaining such records are contained in the Electronic Communications Privacy Act (ECPA), codified in 18 U.S.C. §§ 2701-2711.

Mr. D’Ovidio can be reached via e-mail at dovidio@temple.edu.
Mr. Doyle can be reached via e-mail at jrdoyle@internetcrimes.com.