CHAPTER 15

Cyberpatterns: Criminal Behavior on the Internet

Eoghan Casey

The rather mundane reality is that every new technology can serve as a vehicle for criminal behavior, and the Internet is no exception. The extraordinary dimensions of this new technology, however, are its rapid growth and infinite capacity to make communication both universal and instantaneous. The planet, in a sense, becomes a replicant of the human cortex: billions of neurons synaptically firing at random or in concert, multitasking without interference—prefrontal websites, hemispheric chat rooms, temporal lobe flaming, occipital e-mail.

—Meloy, *The Psychology of Stalking: Clinical and Forensic Perspectives* (1998, p. 10)

CONTENTS

Criminal Profiling: An Introduction to Behavioral Evidence Analysis, Fourth Edition

KEY TERMS

Automated modus operandi
Cyberpatterns
Cybertrails
Dynamic modus operandi
Grooming
Remote assessment
Spoofing

As organizations like IBM focus more energy on projects like the Second Life Virtual World and remotely controlled homes, the interdigitation between the physical and virtual worlds will continue to increase, creating new opportunities for criminal activity. Although it may be some time before we have virtual murders, offenders are currently using the Internet to acquire victims, gather information, fabricate alibis, protect or alter their identities, and communicate with other offenders. Terrorists are making extensive use of computers and the Internet to plan attacks, avoid apprehension, and communicate with the public. For instance, computers played a role in the planning and subsequent investigations of both World Trade Center bombings. Ramsey Yousef's laptop contained plans for the first bombing and, during the investigation into Zacarias Moussaoui's role in the second attack, more than 100 hard drives were examined (*United* States *v. Moussaoui*; *United* States *v. Salameh et al.*; *United* States *v. Ramsey Yousef*). Even traditional violent crimes in which the key forensic evidence is usually physical, such as homicide and sexual assault, can involve digital evidence either directly or incidentally (Reust, 2006a).

CASE EXAMPLE: PREMEDITATED FIRST-DEGREE MURDER

Prosecutors upgraded the charge against Robert Durall, 40, to first-degree murder based on what they described as evidence of premeditation found on his office computer. Durall had been charged with second-degree murder, but a coworker told police he had discovered a number of temporary files on Durall's office computer that showed Durall had conducted Internet searches using key words like kill + spouse, accidental + deaths, smothering, poison, homicides, and murder, according to court documents. A plus sign tells the search engine to pull up only sites that use both terms as key words (*Washington v. Robert A. Durall*, 2003).

Fortunately for investigators, computers record the actions and words of offenders and victims, creating a behavioral archive that can give insight into their thoughts, choices, motivations, interests, and desires. Given its ubiquity and investigative usefulness, investigators must learn to recognize digital evidence and to interpret it from a behavioral standpoint. It might not be obvious, particularly at the outset of an investigation, that a computer or the Internet holds key evidence, so it is advisable to search for potential digital evidence in all cases. This chapter discusses the usefulness of digital evidence in any type of criminal investigation and provides practical guidance for including digital evidence in the deductive criminal profiling process. The predominant focus is on using digital evidence in investigations of violent crime, but a portion of this chapter discusses how criminal profiling may be applied in investigations of computer intrusions and fraud.

CRIME AND COMPUTERS

Not surprisingly, as computers and networks become more prevalent, investigators are encountering an increasing amount of digital evidence of witness, victim, and criminal activity (Casey, 2004). Forensic examination of a floppy diskette that was sent to a television station by the Bind Torture Kill (BTK) serial killer led

investigators to the church where Dennis Rader was council president. In another serial homicide case, investigators tracked down Maury Travis using a map that he had printed from the Expedia Web site and had sent to a reporter in St. Louis to show where another body was located.

A criminal can use the Internet proactively to enhance a modus operandi (MO) or he can use it reactively to avoid detection and capture (Turvey, 2000). For example, John E. Robinson, who referred to himself as "Slavemaster," used the Internet to con some of his victims into meeting him, at which time he sexually assaulted some and killed others (Rizzo, 2001). Robinson first used newspaper personal ads to attract victims and then used the Internet to extend his reach (McClintock, 2001). Robinson also used the Internet reactively to conceal his identity online, often hiding behind the alias "Slavemaster." When Robinson's home was searched, five computers were seized.

The Internet gives offenders greater access to victims, extending their reach from a limited geographical area to victims all around the world. Additionally, the Internet contains a significant amount of personal information about individuals, enabling a predator to search for particular types of potential victims. "One offender might search the Web for potential victims who are involved with church groups or online Bible discussions. Another offender might search for potential victims of a specific age by sifting through personal Web pages or AOL [America Online] user self-descriptions. Sexual predators can lurk in a Usenet newsgroup dedicated to victims of abuse (e.g., alt.abuse.recovery), or they may choose a particular online venue because it attracts potential victims who are located geographically near them" (McGrath and Casey, 2001). Furthermore, by giving offenders access to victims over an extended period of time (rather than just a brief encounter), the Internet enables offenders to gain control of their victims or to gain their victims' trust and possibly to arrange a meeting in the physical world.

In 2000, Lawrence Stackhouse found 15-year-old Diana Strickland's online profile, contacted her using the Internet, and then groomed[1] her until she and a girlfriend agreed to travel to his home in Pennsylvania, where he exploited them sexually for four days until the girlfriend called the police ("Protect Children from Predators on Internet, Parents Tell Congress," 2000). Also in 2000, e-mail and AOL instant messages provided the compelling evidence to convict Sharee Miller of conspiring to kill her husband and abetting the suicide of the admitted killer she had seduced with the assistance of the Internet. Miller carefully controlled the killer's perception of her husband, going so far as to masquerade as her husband to send the killer offensive messages ("Sex, Lies and Murder: *Michigan v. Miller*," 2001). In December 2004, Lisa Montgomery used an Internet chat room to contact 23-year-old Bobbie Jo Stinnett about looking at rat terriers the Stinnetts sold over the Internet. Montgomery later admitted to strangling Stinnett and cutting her open to kidnap her baby.

In late December 2005, 27-year-old Josie Phyllis Brown was reported missing in Baltimore. Digital evidence led investigators to a 22-year-old college student, John Gaumer. Brown and Gaumer met on the Internet site MySpace.com and arranged to meet for a date (Associated Press, 2006). On the night of her disappearance, Brown's mobile telephone records showed that she had talked to Gaumer before meeting with him, and police traced her telephone to a location many miles from where Gaumer claimed to have left her that night. After the web of evidence converged on Gaumer in February 2006, he led police to her body and admitted to beating Brown to death after their date. Gaumer used the Internet extensively to communicate with and to meet potential dates. Part of the evidence against him was a digital recording of "thumping noises, shouting and brief bursts of a woman's muffled screams" apparently created when

[1] Grooming is a general term used to describe the process by which a sexual predator gains control over his victim. According to Johnson (1997), "Perpetrators attempt to build both a trusting and fear-based relationship with their victim, with an end goal of being able to get sexual contact without significant resistance."

Gaumer's mobile phone inadvertently dialed Brown's phone number (McMenamin, 2007). In his confession to police, Gaumer stated that he removed her nose, jaw, teeth, and most of her fingertips in an attempt to thwart identification of her body and that he later sent an e-mail to her account to make it appear that he did not know she was dead.

CYBERTRAILS

Everyday activities leave a significant amount of digital data lying around. Third parties, such as mobile telephone providers, banks, credit card companies, and electronic toll collection systems, can reveal significant information about an individual's whereabouts and activities and are a staple source of evidence for criminal investigators.

Even when they are not consciously using networks, offenders and victims leave digital footprints as they move through the world, creating cybertrails that an investigator may be able to retrace to reconstruct where they were and what they were doing at particular times. For example, records from a missing person's mobile telephone provider or car navigation system may indicate where the person went and when.

Similarly, the computers and other digital devices, including cell phones and PDAs, that people use at home and work contain remnants of documents, photographs, Internet communications, and other details that generally reveal a great deal about their daily life, inner thoughts, and motivations. For example, Web browsers on a computer often maintain a list of all pages that have been viewed and can temporarily store recently viewed content in a cache to improve performance. This cached data can include Web-based e-mail and other activities that may be useful to investigators. Data that have been "deleted" often remain on a computer indefinitely and may be recoverable using digital forensic techniques and tools. Information posted on the Internet that an individual later altered or removed may also be recoverable through archives like the Way Back Machine (www.archive.org).

Handheld devices may contain entries or photographs that capture ongoing criminal activity or indicate where the victim was or whom she met with at a particular time. In an alleged rape case, a forensic examiner recovered cell-phone video that showed Dominic Jones having sex with a woman who had apparently passed out after drinking (Chanen and Xiong, 2007).

Various log files on servers may provide useful evidence in a case involving the Internet. For instance, sending an e-mail usually generates a record of the sender's location at a particular time, leaving traces on the device used by the sender, intermediate e-mail servers, and the recipient's computer. Therefore, in addition to looking for the contents of e-mail, an investigator can determine what messages passed through the system. If a message has been deleted to conceal a crime and cannot be recovered, there may still be evidence of its existence in the server's log files. Additionally, many e-mail server logs contain information about when individuals checked their e-mail, potentially recording their whereabouts at a particular moment.[2]

The detailed and personal nature of information that may be available on the Internet is demonstrated by the online statements and interactions between Taylor Behl and Ben Fawley (Bardsley and Huff, 2007). Behl went missing on September 5, 2007, and her body was found a month later in an isolated rural area that Fawley was familiar with. Fawley subsequently admitted to killing Behl and was convicted in August 2006. Behl's postings on Livejournal.com using the nickname "tiabliaj" were akin to online diary entries describing

[2] An e-mail program can be configured to periodically download e-mail automatically without requiring the user to be present at the keyboard. This emphasizes that care must be taken when interpreting digital evidence and attributing online activities to an individual.

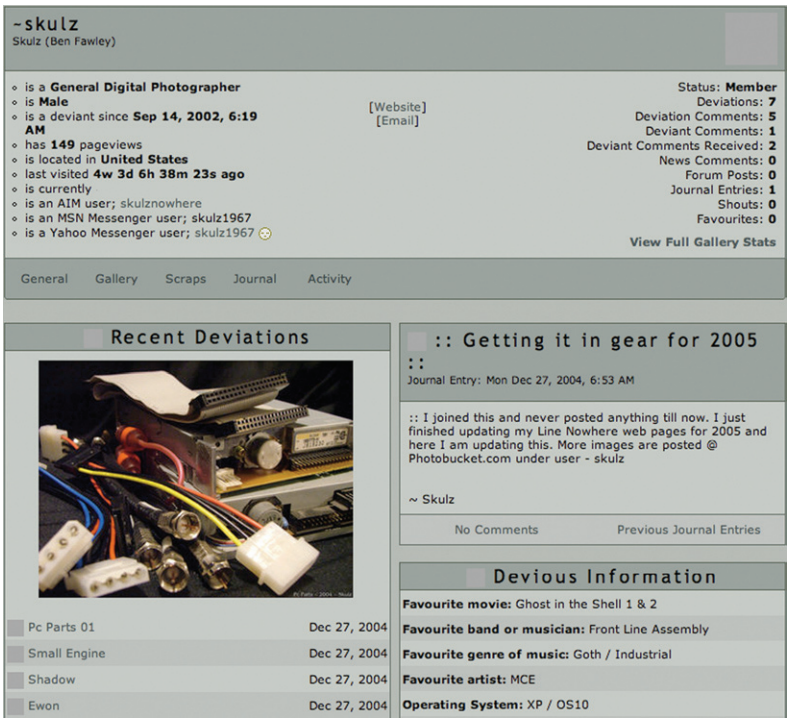

FIGURE 15.1
Ben Fawley's Web page on deviantart.com showing interests and computer-related information.

her thoughts and personal life, including interactions with Fawley. Fawley maintained a number of Web pages that contained a variety of information about him (Figure 15.1). The information in Figure 15.1, from one of Fawley's Web pages, includes various Internet accounts with the name "Skulz," a photograph of computer parts, and an indication that Fawley used both Windows and Macintosh operating systems. Another Web page that Fawley maintained under the nickname "line-nowhere" indicated that he had a number of computers: "I use MSIE on five of my PC's. I have Safari on the crapMac, but I have just added Firefox to three of my PC's as I find MSIE is a royal pain in the ass." When police searched Fawley's home, they seized significant amounts of computer equipment and storage media, as well as digital cameras and mobile telephones.

As the following examples demonstrate, while sexual predators exploit the Internet to identify and attract victims and facilitate their crimes, criminal investigators can exploit their associated cybertrails to track the whereabouts of the perpetrators and document their activity:

- A sexual predator might frequent AOL chat rooms because AOL has a high percentage of new Internet users who are not yet familiar with the risks of this new medium. Locating and examining the offender's AOL account could lead to valuable digital evidence. Recording all of the offender's chat sessions could result in a wealth of behavioral evidence.
- A sexual predator might frequent a local chat room to gain access to local victims. Determining that the offender is located in a certain area significantly limits the suspect pool. Monitoring chat rooms that attract individuals from that geographic area may lead to the offender or other victims.

- A sexual predator might frequent Usenet (alt.abuse-recovery, alt.teen-advise, alt.torture) looking for a specific kind of victim expressing particular vulnerabilities. A search of Usenet archives may lead to useful information about the offender.
- A sexual predator might post online personal ads or use online dating services to acquire a certain kind of victim. The ad/dating service may have log files containing the IP address(es) that the suspect used to post information or may have records that lead to other victims.

Even if digital evidence does not contain the "smoking gun," it can reveal actions, positions, origins, associations, activities, and sequences useful for reconstructing the events surrounding an offense (Casey, 2006). Therefore, whether computers and networks are involved directly or indirectly, it is productive for investigators to view cybertrails as an extension of the physical world, as opposed to a completely irrelevant and separate space. Taking this viewpoint enables investigators to incorporate cybertrails and the associated digital evidence into the investigative reconstruction process detailed in this text.

The primary assumption in deductive criminal profiling is that the choice of victims, the choice of crime scenes, and the actions of an offender in executing a crime provide telling information about the perpetrator. This assumption can be applied to cybertrails because (1) computers and networks are an extension of, and another means to mediate, the physical world; and (2) computer technology does not fundamentally change human behavior, but instead is simply a tool that facilitates, and captures virtual instances of, activity. An individual may do things on the Internet that he or she would not do in the physical world, but those online activities are still recognizable as, and reflective of, that person's behavior.

Just as following an offender's cybertrails can improve a profile, the profiling process can direct investigators to additional sources of digital evidence, as the following case examples demonstrate.

CASE EXAMPLE: DEATH THREAT

An individual was receiving anonymous threatening e-mail messages that made her fear for her life. The messages were sent through an anonymous e-mail service, making it difficult for investigators to identify the sender or origin of the messages. However, information contained in the messages suggested that the sender was in the same organization as the victim. Investigators believed that the sender would have initially sent himself a test message to ensure that no identifying information was disclosed in the e-mail header. The log files of the organization's e-mail server showed that one other individual in the organization had received a message from the same anonymous e-mail service. When this individual's computer was examined, an abundance of digital evidence was found indicating that he was responsible for the threatening e-mail.

CASE EXAMPLE: BLACKMAIL

In an extortion case, the offender sent a message to the victim from a Web-based e-mail account. The Internet protocol (IP) address contained in the e-mail header showed that the message was sent from a computer located in an Internet café, but investigators were unable to determine who was using the computer at the time. Believing that the offender may have checked the Web-based e-mail account for responses to his message, investigators obtained all records relating to that account from the Internet service provider. These records indicated that the offender had indeed connected to the e-mail account from his home computer.

CASE EXAMPLE: CHILD EXPLOITATION

Behavioral analysis of a sexual predator directed undercover investigators to particular online chat rooms that the offender trawled for victims and enabled investigators to pose as the type of victim that attracted the offender.

Digital evidence may be scattered across different media sources and in multiple online sites, and a profile of the perpetrator may help investigators identify other investigative steps to find additional sources of evidence. For example, if a profile indicates that the current victim probably was not the first to be targeted by the offender, investigators will be motivated to seek evidence relating to other victims. A profile may also suggest to investigators what types of victims to look for and where the offender might have come into contact with them.

As offenders become more aware of digital forensic techniques, they are employing concealment tools and techniques, such as encryption, misleading file names, or disk wiping. Therefore, it is important for a profiler to consider when digital evidence should be present but is absent. Given such direction, a trained forensic examiner may be able to recover and use these data to reveal evidence that a criminal sought to hide, and the examiner may thereby glean a great deal about an individual's activities.

PROFILING COMPUTER CRIMINALS

To date, the majority of efforts to apply profiling to crimes involving computers has focused on criminals who target computers. In one study, computer criminals were split into the following categories (Icove, Seger, and VonStorch, 1995):

- Computer crackers: groups and individuals
- Computer criminals: espionage and fraud/abuse
- Vandals: strangers and users.

In another study, hackers were stereotyped as white, middle-class, obsessive antisocial males between 12 and 28 years old, with an inferiority complex and a possible history of physical and sexual abuse (Rogers, 1999). Several other attempts have been made to create general profiles of computer criminals using information from media reports, offender interviews, and anecdotal observations.

Although these efforts to create inductive profiles give a general overview of past offenders and may be useful for diagnosing and treating associated psychological disorders, they are of limited use in an investigation. In fact, such generalizations about criminals may be misleading, prompting investigators to make incorrect assumptions about an offender. Since investigators usually require particulars rather than generalizations, criminal profiles should contain specific conclusions, substantiated by evidence. If a generalization is deemed necessary, it should be made with great care and extensive research or it is likely to be unhelpful in an investigation.

Studying past crimes can help investigators assess offenders and their motives and make strategic decisions in an investigation. Researchers concerned with computer-related crime have focused on dangerous critical information technology insiders (CITI)—individuals who threaten critical infrastructures from within an organization (Shaw, Ruby, and Post, 1998). This research focuses on threat assessment, attempting to predict the future behavior of high-risk individuals to mitigate the damage they might cause. According to this research, all CITIs have one common trait—introversion, which makes them "less likely to deal with stress

in an overt, constructive manner, and less likely to seek direct assistance" (Shaw, Post, and Ruby, 1999). CITIs are also more likely to express their problems via e-mail than in person. Studies have identified six high-risk characteristics: a history of personal and social frustrations, computer dependency, ethical flexibility, reduced loyalty, a sense of entitlement, and a lack of empathy. These studies also provide several motivational categories in an effort to help identify and evaluate the risks associated with problem individuals (Table 15.1). These motivational categories overlap with those mentioned in Chapter 13: power reassurance (compensatory), power assertive (entitlement), anger retaliation, and profit oriented.

More recent empirical studies provide additional insight into computer crimes committed by individuals within an organization. In studies by the Secret Service/Carnegie Mellon University Software Engineering Institute (Keeney et al., 2005; Randazzo et al., 2004) and the Defense Personnel Security Research Center (Shaw and Fischer, 2005), the majority of the crimes surveyed had a profit motive, with some level of anger retaliation. Although the criminal activity was committed using computers, the method of attack was often nontechnical, generally taking advantage of the business to embezzle funds. The importance of digital evidence in these investigations was perhaps lower than one might expect, emphasizing the need to combine digital forensics with traditional investigative techniques like criminal profiling. In 74% of the cases surveyed, system logs helped identify the insider, while in 30% of the cases forensic examination of the targeted network, system, or data helped identify the subject.

Table 15.1 Motivational Categories of Critical Information Technology Insiders

Category	Motivational Descriptive Summary and Demonstrative Example
Explorers	Motivated by curiosity, rarely cause purposeful damage. Example: Idle employees access poorly protected network resources that they are not officially authorized to access.
Good samaritans	Motivated by a desire to "save the day" or to show off their abilities. Example: A system administrator on one system identifies a vulnerability on another system that is not the administrator's responsibility and breaks into the vulnerable system to fix it rather than informing the responsible system administrator.
Hackers	Motivated by a need to bolster self-esteem by violating access boundaries. Example: An individual connects his employer's secure network to the Internet in violation of policy, providing his friends on the Internet with access to the secure system and sensitive information it contains.
Machiavellians	Motivated by personal gain, damaging people and systems to achieve their goals. Example: An individual who enjoys traveling introduces malfunctions in her employer's equipment abroad so that she will be sent to other countries to repair the systems.
Exceptions	Believe that they are special and entitled to special treatment. Example: A system administrator has unique knowledge of an organization's computer systems and feels that he deserves better pay, benefits, and treatment than other employees.
Avengers	Motivated by specific perceived wrongs. Example: A system administrator hears that she is going to be laid off, so she encrypts patient files and holds them ransom in the hope of getting a better severance package.
Career thieves	Motivated by profit. Example: An individual embezzles money using an organization's computer system.
Moles	Motivated by profit but indirectly through espionage. Example: An individual who joins an organization with the express purpose of obtaining proprietary information that he can sell to competitors.

Psycholinguistic Analysis of Digital Communications

Shaw's more recent work has expanded from managing insider threats to using deductive profiling techniques in active investigations involving unknown offenders (Shaw, 2006, p. 26). Shaw uses a methodology called remote assessment and performs content analysis to extract information from written and spoken communications:

> Remote assessment refers to a portfolio of methods used to evaluate individuals and groups when direct contact methods (interviews, questionnaires, etc.) are not feasible or desirable. Sometimes referred to as Unobtrusive Methods, these techniques have been used by researchers concerned about disturbing the natural environment of their subjects.

Shaw's approach is useful when investigators have e-mail messages, Internet chat logs, or recorded audio that captures the offender's words. E-mail messages, newsgroup posts, and other online statements may contain unusual or repeated verbal behaviors or show a level of planning and forethought related to a criminal act. Software that implements psycholinguistic analysis has been developed to process electronic communications and to highlight noteworthy characteristics for a human analyst to evaluate (Shaw and Stroz, 2004).

In addition to psycholinguistic analysis of content, Shaw's remote assessment methodology takes into account the context of communications. The target, delivery method, time, related organizational events, and other context can give the profiler a better understanding of the offender and may reveal useful patterns of behavior. For example, an offender who attacks just before a company goes public may be attempting to harm the company financially. As another example, an offender's use of concealment technology when communicating shows technical sophistication and may suggest that the offender is known to the victim. This type of assessment can give insight into the offender's motives, state of mind, psychological disorders, and distinctive verbal behavior, such as unusual word usage or errors in spelling, that may help narrow the suspect pool. When dealing with an insider, such as an ex-employee, it may be possible to compare writing samples of potential suspects.

CASE EXAMPLE: ANGRY INSIDER

Each board member of a company received an anonymous letter viciously disparaging the CEO and aspects of the company's operations, citing details that could only be known to an insider. Because of fears that the information in the letter might be made public and circulated to suppliers and customers, an investigation was launched to identify the sender. After analyzing the profile of the author, a suspect pool of insiders was identified, and e-mail and other writings were compared to the anonymous letter writer, resulting in not only the sender's identification but also a method for managing his relationship with the company to mitigate the risk of further harm.

DIGITAL BEHAVIOR OF UNKNOWN OFFENDERS

Criminal profiling can be most useful when little is known about the offender(s), which is particularly important when offenders use the Internet to conceal their identities and activities. Criminal profiling assists investigators by:

- Distinguishing whether a single offender committed multiple crimes or multiple offenders are involved

- Providing likely offender characteristics to aid the technical investigation
- Identifying likely suspects from a given pool based on offender skill level, access to victim/target, and other technical characteristics
- Revealing modus operandi and signatures to help investigators search for related behaviors and to assess offender motivations
- Giving insight into offender motivations and general psychological state
- Assessing the dangerousness of offenders
- Revealing additional sources of evidence

In one case, a company and its customers were harassed by embarrassing e-mails containing derogatory information about the company and disturbing sexually explicit attachments that were spoofed to appear that company executives were the senders. After two years of repeated spoofed e-mail attacks, it remained unclear whether the perpetrator was an individual or a group, an insider or outsider, or even what the offender(s) wanted in order to stop their harassment.

Behavioral analysis of the harassing communications showed that one individual with a high technical skill level was responsible for all of the activities, and it indicated that the subject was a highly intelligent male over 30 who was extremely angry with the target company. This information led to further investigation of other anonymous contacts that had not previously been associated with the perpetrator of the harassing e-mail attacks. E-mail communications were established with the perpetrator and, with the assistance of a behavioral psychologist, additional information about the perpetrator was elicited from him about his motivation, culminating in a cyber-extortion demand. In the negotiations over the extortion demand, the perpetrator's state of mind was regularly assessed to evaluate the level of danger he posed to others.[3]

In this investigation, digital forensic analysis of the company's computer systems uncovered no evidence that the perpetrator was a malicious insider, but it did identify suspicious connections from computers at a nearby university, providing investigators with a solid lead and confirmation of an outside hacker. As suggested by the profile, the offender was technically skilled enough to conceal his identity by using publicly accessible computers at university computer laboratories and wireless access points. Subsequent surveillance of the locations used by the offender to send spoofed e-mails led investigators to a prime suspect who matched many of the characteristics detailed in the profile. Because the profile indicated that the offender might be dangerous and mentally unstable, investigators were cautious when they ultimately apprehended him. This case demonstrates how behavioral analysis of the digital evidence can provide investigators with information about the numbers of individuals involved in the criminal activity, the skill level of the individuals involved, other evidence that is actually related though may not superficially appear to be, and the physical security risk that the perpetrator poses.

An offender's online activities may also indicate that the offender is taking precautionary measures to avoid identification and apprehension. For instance, some offenders protect themselves by using computer-smart nicknames, such as "En0ch|an" instead of "Enochian." Because a search engine does not realize that the zero represents an "o" and the pipe (|) represents an "i," a search for "En0ch|an" will not find information labeled with "Enochian."[4] Additionally, offenders may use anonymous or forged e-mail messages to conceal their identities. Investigators should determine how much technical knowledge was required to perform such a task and whether every modification was necessary to conceal the person's identity or whether the

[3] For further description of this case, see Howell (2006) and Shaw (2006).
[4] To make matters worse, some search engines treat a pipe (|) as a separator and may therefore search for terms other than those specified.

modifications were instead created to fulfill a psychological need of the offender. Explaining how and why the offender conceals his or her identity may lead investigators to identifying information that the offender failed to hide or may help investigators narrow the suspect pool (e.g., to people who were intimately familiar with the victim and concealed their identify to avoid recognition by the victim).

CASE EXAMPLE: INTERNAL OFFENSE

A large company received an anonymous letter containing documents from an executive's computer. In addition to the concerns raised by the documents, the fact that someone was able to obtain access to these sensitive materials without the executive's knowledge raised security concerns. If the anonymous whistle-blower had gained unauthorized access to the executive's computer system or e-mail, this would have to be considered. A behavioral assessment helped focus the investigation on a person morally offended by the executive's activity, which was the subject of the documents and was a violation of corporate policy. The behavioral analysis of the anonymous whistle-blower's activities on the company's computer systems also supported the assessment that the security breach was specifically targeted at the executive and his activities and was not more far-reaching.

Feeling protected by some level of anonymity, individuals often do things on the Internet that they would only imagine doing in the physical world and express thoughts that they would otherwise keep to themselves. Digital evidence may also contain information that can be used to determine the offender's sex, age, occupation, interests, relationship status, and other potentially useful information. An offender's Web site and online presence can give the viewer an impression of the offender's self-image, state of mind, interests, and more. The choice of online nicknames can be revealing (e.g., Slavemaster, Zest, Dr. Evil), and an offender's Web pages may contain stories that give insight into his or her motives and fantasies and may have links to favorite areas online that can lead to other victims and additional evidence. This last point also applies to the physical world—an offender's Web page may contain references to, or photographs of, favorite locations that can be useful when looking for other potential victims or sources of physical evidence.

CASE EXAMPLE: CHILD EXPLOITATION

An offender's admissions about state of mind, sexual fantasy, or personal/sexual conflict can provide insight into his or her behavior and motivations. For instance, in one traveler[5] case, a profiler examined the offender's online activities and concluded that the offender believed he was genuinely in consensual relationships with his young victims. "He sees nothing about his behavior as criminal or exploitative. He believes that he is merely seizing the day, and that what he is doing benefits the children he exploits. His motive is not to physically harm his victims but to be loved and admired by them. He confuses his own identity with theirs, to an extent, projecting a childlike affect to them. An interview strategy that exploits these factors by being sympathetic to them will be successful in getting the most information from this suspect."

[5] A sexual predator who obtains victims online and then travels to meet them is commonly called a traveler.

MANAGING OFFENDER BEHAVIOR

An effective profile can help investigators decide whether attempts to contact and to communicate with the offender would be useful or harmful, and how to best approach the offender. It can also be helpful to know that certain sex offenders will confess to their crimes when treated in a certain manner, but the same approach may drive others into deeper denial.

In the same case involving the spoofed e-mails noted earlier, investigators decided to send an e-mail with a Web bug in an effort to learn more about an unknown offender. However, a profiler working on the case determined that the offender was highly skilled and would most likely notice and circumvent the tracking mechanism embedded in the e-mail. The profile also noted that the suspect was exhibiting signs of mental instability and was potentially dangerous. When law enforcement officers served a warrant at the suspect's home, they found not only digital evidence connecting him with the offense but also firearms and the recipe and ingredients for a poisonous toxin called ricin.[6]

VICTIMOLOGY

Given the growing number of people encountering and communicating with each other on the Internet, it is necessary to consider the possibility that the offender had contact with the victim using the Internet. For instance, during the investigation of Robinson, cooperation between law enforcement agencies overcame potential physical linkage blindness, and victims' bodies were located in two neighboring states (McClintock, 2001). Additional investigation of the offender's activities, combined with interviews of online witnesses, may reveal that an offender communicated with other victims on the Internet who have not yet been identified. Conversely, in the case of missing victims, a thorough analysis of their computers might lead to a common offender. Therefore, as a rule, victimology should include a thorough search of the Internet, pertinent computers, and handheld devices.

For example, suppose the victim in a homicide accesses the Internet through Verizon and uses her Verizon e-mail account to communicate with friends and family, but uses Google Mail to communicate with strangers. Her computer would contain e-mail from friends and family but might contain nothing to or from the strangers she encountered on the Internet. Of course, the diligent investigator would examine the victim's Web browser history, see the many connections to gmail.com, and obtain the victim's messages from Google.

In addition to exploring the possibility of an Internet link between the victim and offender, try to gain some understanding of the victim as an individual from his or her Internet activities. Every detail about the victim's life and behavior contributes to one's understanding of why that particular individual became a victim of a crime. Try to determine the what, why, where, how, and when of the victim's Internet activities by asking questions like the following:

- Did the victim have Web pages, post to Usenet regularly, use chat networks, or send/receive e-mail or text messages on a mobile phone? The contents and context of any such online activities help a profiler understand the victim.
- Did the victim use a parent's account, a personal account, or an anonymous account? If the victim was using an anonymous account, was he or she hiding from someone (e.g., abusive ex-boyfriend)?
- What did the victim get from the Internet that was not accessible otherwise (e.g., friendship, drugs, fantasy fulfillment)?
- Where did the victim access the Internet (e.g., at home, work, a café or bar)? Why did the victim pick that location to access the Internet (e.g., privacy, business, or to meet people face-to-face)?

[6] For further description of this case, see Howell (2006) and (Shaw 2006).

- Did the victim exhibit any behavior that sheds light on his or her mental state, sexuality, lifestyle, intelligence, or self-image? For example, was the victim involved with bondage and sadomasochism (BDSM) online groups?
- Are there discernible patterns in the victim's Internet activities that suggest habits or schedules? Were there any breaks in these patterns around the time of the crime?

When looking for information on the Internet, investigators should not limit themselves to computer queries. Interviewing individuals with whom the victim interacted on the Internet can uncover online nicknames and areas of the Internet that the victim used. A person's private online hangouts can be the most revealing from a victimology standpoint and may be the way the offender crossed cybertrails with the victim.

CASE EXAMPLE: HARASSMENT

A woman was being harassed and threatened over the Internet, primarily via a Hotmail account. The victim put a significant amount of personal information on the Internet, such as her age, home phone and address, background, photographs, and personal interests. The offender used a pseudo-anonymous e-mail account to hide his identity but did not have enough knowledge of the Internet to realize that the e-mail account did not provide complete anonymity (Hotmail headers contain the IP address of the sender's computer). Although the offender claimed to have located the victim through her Web page, he exhibited a high degree of familiarity with the victim's surroundings (e.g., town, residence), suggesting that he spent a significant amount of time in the area. Additionally, the offender did not suggest a face-to-face meeting and did not use the victim's phone number although it was provided on her Web page, perhaps because he was concerned that the victim would recognize or be repelled by him if they met or spoke. Perhaps the offender knew the victim or felt less confident/comfortable communicating in person. The e-mail messages contained some descriptions of the offender's fantasies and suggested a degree of mental instability.

It is also important to include digital evidence when assessing victim risk. Risk assessment on the Internet works in the same way as in the physical world, as the comparisons in Table 15.2 demonstrate.

Table 15.2 Analogous Risks in the Real and Virtual Worlds

Risk	Physical World	Internet
High-risk victim	Unattended child who talks with strangers while walking home from school	Unattended child in an Internet chat room who talks with strangers
High offender risk	Offender who acquires victims in an area that is surveyed by security cameras	Offender who acquires victims in an area of the Internet that is monitored or recorded
Low-risk victim	Individual who avoids going into certain areas unaccompanied and does not give personal information to strangers	Individual who avoids certain areas of the Internet and does not give personal information to strangers
Low offender risk	Offender who wears a mask and performs covering behavior to avoid detection	Offender who uses anonymity provided by the Internet and performs covering behavior to avoid detection

The Internet can influence victim risk, putting an otherwise low-risk victim at high risk of certain crimes. For example, if a woman makes a large amount of personal information available on the Internet and participates in online activities that expose her vulnerabilities, this can increase her risk of being stalked. If a woman who is reserved and cautious in the physical world uses the Internet to explore bondage and torture fantasies and arranges to meet an online acquaintance to act out these fantasies, this online activity can increase her risk of being raped or killed.

CASE EXAMPLE: TYPE "M" FOR MURDER

Sharon Lopatka traveled from Maryland to North Carolina to meet her killer. Friends described Lopatka as a normal woman who loved children and animals. Lopatka's activities on the Internet give a very different impression, however. Lopatka was evidently interested in sex involving pain and torture. Victimology that did not include her Internet activities would have been incomplete, lacking the most relevant aspects of her character and would probably describe her as a low-risk victim when, in fact, she was quite a high-risk victim. For instance, in the murder of Sharon Lopatka, the victim's home computer contained hundreds of e-mail messages that provided the crucial link between the victim and the murderer, Robert Glass. Before these e-mails were found, investigators believed that they were dealing with a low-risk victim, and without these e-mails, it is unlikely that the investigators would have found the offender.

Individual pieces of digital data may not be useful on their own, but patterns of behavior can emerge when the pieces of digital evidence are combined. A victim might always check e-mail at a specific time or might always frequent a particular area on the Internet. A disruption in this pattern could be an indication of an unusual event—determining what that event was could generate a key lead. If there was no break in the victim's routine, this consistency may help investigators hypothesize that the offender was aware of the victim's routine and planned the crime accordingly or that the offender happened upon the victim and took advantage of an opportunity. Discerning such patterns can be challenging when digital data are involved because there is often a massive quantity of information. Therefore, a thorough forensic analysis should always be performed to provide familiarity with the complete body of evidence and the opportunity to consider all possibilities before getting caught up with one detail or theory.

DEDUCTIVE PROFILING OF COMPUTER INTRUDERS

The same techniques discussed in this chapter can be useful for crimes committed on, not just using, computers, such as data breach cases and network intrusions. When an offender uses the Internet to commit crimes, it can be difficult to pinpoint all of the relevant evidence in the digital vastness. Knowledge of a criminal's MO and signature is very useful when scouring the Internet for information regarding a case because it gives investigators a clearer sense of what to look for and where to look. The Internet, however, has many areas that are private and may never show up in a routine search. Sometimes an offender's MO or signature will indicate that he uses one or another of these out-of-the-way places. Developing an understanding of the offender's MO can direct investigators to look for particular traces of digital behavior or to monitor particular virtual areas where the intruder is likely to appear.

CASE EXAMPLE: COMPUTER INTRUDER CAUGHT IN THE ACT

In a computer intrusion/information theft case, investigators determined how the offender operated and what he was looking for by carefully examining the compromised computers. Investigators used this knowledge to identify and monitor other machines on the network that would attract the intruder. After several hours, the intruder was detected on one of the systems being monitored, giving investigators one of the most vivid forms of evidence, a live recording of a crime in progress. While monitoring the intruder, investigators were able to determine that he was a recently fired employee who was dialing into the network from his home. They quickly obtained a search warrant for his personal computer and found copies of the stolen information on the hard disk.

For an in-depth example of MO and signature in the context of computer crime, consider the well-known case of Kevin Mitnick. Mitnick had an advanced MO that made it difficult to track him down. He would break into telephone networks, create a clever dial loop to hide his whereabouts, and use a cellular phone to dial into a large Internet service provider. He would then use advanced techniques to break into computers and steal software, credit cards, and data. A team that consisted of computer expert Tsutomu Shimomura and the FBI finally tracked Mitnick down using cellular-frequency direction-finding antennae. Although Mitnick's main motivation seemed to be profit, he exhibited some other behaviors that were clearly not necessary to commit crimes (i.e., signature behaviors). For example, in addition to breaking into Shimomura's computer and stealing advanced computer software, Mitnick allegedly left taunting voice messages on Shimomura's voicemail, possibly as a form of power reassurance (www.takedown.com/evidence/voicemail).

An interesting aspect of MO in the context of computers arises when criminals take advantage of computer automation during the commission of a crime—automated actions and offender behavior can be difficult to differentiate. Automation can be particularly problematic when several criminals use the same automated tools. For example, programs exist that automate certain methods of breaking into computer systems and hiding incriminating evidence, providing an automated modus operandi that makes multiple offenders almost indistinguishable. When every crime scene looks almost identical, it becomes more difficult to link cases committed by a single offender and to understand the unique motivations of different offenders.

To make case linkage even more difficult, offenders who use the Internet can change their modus operandi with relative ease. As offenders become more familiar with the Internet, they usually find new ways to make use of it to achieve their goals more effectively. An offender who uses the Internet creatively can change his or her modus operandi so frequently and completely that it is best described as dynamic. For instance, individuals who break into well-secured computer systems may have to develop a novel intrusion plan for each unique target. A dynamic modus operandi has also been seen when an offender is consciously trying to foil investigators. For instance, when a stalker becomes aware that investigators are preventing one method of terrorizing the victim (e.g., e-mail), he or she uses another method (e.g., ICQ).

Investigators who are able to extract key behavioral information from available digital evidence and who can make sound deductions based on that behavioral evidence are invaluable in an investigation involving the Internet. Determination of motivation and intent can be critical when available evidence does not provide a complete picture of the offender's actions. For instance, in data breach cases, one of the main questions that arises is whether the intruders gained access to confidential data stored on the compromised computer. When it is not possible to prove that the intruders did not access the data of concern, an assessment of their activities can reveal that their intent was not focused on the confidential data but rather to use the computer system for some other purpose, such as storage of contraband or to launch attacks against other systems on

the Internet (Casey, 2003). In one case, forensic examination of the target systems found that the motivation for computer breach was not to steal sensitive data but to find storage space for pirated movies (Reust, 2006b). Additionally, investigators who can recognize signature behaviors in a digital setting are in a solid position to overcome the challenges of automated or dynamic modus operandi—they can use signature behaviors to link cases and make deductions about offenders.

Like an autopsy, the forensic analysis of the target computer systems will reveal a significant amount about an attack (Casey, 2004). However, it is important for investigators to realize that there may be other computers that contain significant amounts of relevant digital evidence. Just as a crime in the physical world can have multiple crime scenes, computer intrusions can have primary and secondary scenes, each containing potentially useful information. Computer intruders often perform surveillance of a target computer from one location, move (virtually) to another location on the network to break into the target system (potentially passing through several intermediate systems), gain unauthorized access to the target system and steal money or information, destroy the target system and all of the evidence it contains, and delete evidence on other systems that were used during the commission of the crime. A staging area used by a computer intruder may contain evidence related to the crime, tools left by the offender, and communications with cohorts, and could provide a link between an individual and the primary crime scene.

It can also be productive to perform a kind of victimology relating to the target computer(s) in an intrusion case. In crimes where computers are the targets, the underlying question is the same: Why did the offender choose the target computer, and what was the risk the offender was willing to take? Consider a well-protected computer, for example. If an offender overcomes many obstacles and exposes himself or herself to many risks to break into the computer, this ability may indicate that the offender was familiar with the target system, had a strong desire for something on the target system, and was skilled enough to overcome the obstacles and risks.

To assess victim risk when the target is a computer, gather information about the computer, including the make and model, the operating system, where it was located, what it contained, who had access to it, what other computers it regularly connected to, and how difficult it was to break into. Determine whether there were any previous unsuccessful attempts to access the computer. If an offender required a significant amount of knowledge about the target computer system to commit the crime, investigators should try to determine how this knowledge was obtained. Was it available only to employees of an organization? Could the offender have obtained the information through surveillance, and if so, what skill level and equipment were required to perform the surveillance?

In investigations of computer intrusions or violent crime, computers and the Internet may contain crucial information about the people involved. Profiling can utilize this rich repository of digitized human behavior to aid an investigation and can direct investigators to other potential sources of digital evidence that might otherwise be overlooked.

SUMMARY

As computers and networks become more prevalent, investigators are encountering an increasing amount of digital evidence of witness, victim, and criminal activity. A criminal can use the Internet proactively to enhance his current modus operandi or he can use it reactively to avoid detection and capture. Additionally, the Internet gives offenders greater access to victims, extending their reach from a limited geographical area to victims all around the world.

Everyday activities leave a significant amount of digital data lying around, especially from third parties, such as mobile telephone providers, banks, credit card companies, and electronic toll collection systems. Consequently, even when they are not consciously using networks, offenders and victims leave digital footprints as they move through the world, creating "cybertrails" that an investigator may be able to retrace to reconstruct where these computer users were and what they were doing at particular times.

To date, the majority of efforts to apply profiling to crimes involving computers have focused on criminals who target computers. Although these efforts to create inductive profiles give a general overview of past offenders and may be useful for diagnosing and treating associated psychological disorders, they are of limited use in an investigation. They can even be misleading.

Criminal profiling can be most useful when little is known about the offender(s), which is particularly important when offenders use the Internet to conceal their identities and activities. Feeling protected by some level of anonymity, individuals often do things on the Internet that they would only imagine doing in the physical world, and they express thoughts that they would otherwise keep to themselves. Digital evidence may also contain information that can be used to determine the offender's sex, age, occupation, interests, relationship status, and other potentially useful information.

When an offender uses the Internet to commit crimes, it can be difficult to pinpoint all of the relevant evidence in the digital vastness. The Internet, however, has many areas that are private and may never show up in a routine search. Sometimes an offender's MO or signature will indicate that he or she uses one or another of these out-of-the-way places. Developing an understanding of the offender's MO can direct investigators to look for particular traces of digital behavior or to monitor particular virtual areas where the intruder is likely to appear.

Questions

1. True or False: Hackers are mostly teenagers who play video games and have too much time on their hands.
2. Explain how an automated modus operandi is made possible.
3. Cybertrails are often created passively. Give three examples of how this might occur.
4. What is the purpose of a dynamic modus operandi?
5. Why might a predatory sex offender troll America Online (AOL) for victims, as opposed to somewhere else?

ACKNOWLEDGMENTS

The author thanks Brent Turvey for his efforts to enhance the body of knowledge in forensic science and crime reconstruction. The author also thanks his colleagues at Stroz Friedberg, LLC, in particular Beryl Howell and Eric Shaw, for their ongoing support.

REFERENCES

Associated Press, 2006. Police Charge Md. Student in Murder: UMBC Student Met Woman on MySpace.com, February 9.

Bardsley, M., Huff, S., 2007. Disappeared: Taylor Behl, Crime Library. Court TV . Available at www.crimelibrary.com/criminal_mind/forensics/taylor_behl.

Casey, E., 2003. Determining Intent: Opportunistic vs. Targeted Attacks. Computer Fraud & Security (4), 8–11.

Casey, E., 2004. Digital Evidence and Computer Crime: Forensic Science and the Internet, second edition. Academic Press, London, England.

Casey, E., 2006. Reconstructing Digital Evidence. In: Chisum, J., Turvey, B. (Eds.), Crime Reconstruction. Academic Press, London, England.

Chanen, D., Xiong, C., 2007. To a New Kind of Sleuth, Phones Leave a Rich Trail. Minneapolis *Star Tribune* (July 22).

Gudaitis, T., 1998. The Missing Link in Information Security: Three Dimensional Profiling. Cyberpsychological Behavior 1 (4), 321–340.

Howell, B., 2006. Real World Problems of Virtual Crime. In: Balkin, J. (Ed.), Cybercrime: Digital Cops in a Networked Environment. New York University Press, New York, NY, pp. 95–98.

Icove, D., Seger, K., VonStorch, W., 1995. Computer Crime: A Crimefighter's Handbook. O'Reilly & Associates, Sabastapol, CA.

Johnson, S., 1997. Psychological Force in Sexual Abuse: Implications for Recovery. In: Schwartz, B.K., Cellini, H.R., Kingston, N.J. (Eds.), The Sex Offender: New Insights, Innovations and Legal Developments, vol. 2. Civic Research Institute, Kingston, NJ, pp. 17-1–17-11.

Keeney, J., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., Rogers, S., 2005. Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. National Threat Center, U.S. Secret Service, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, Washington, DC; Pittsburgh, PA.

McClintock, D., 2001. Fatal Bondage. Vanity Fair June.

McGrath, M., Casey, E., 2002. Forensic Psychiatry and the Internet: Practical Perspectives on Sexual Predators and Obsessional Harassers in Cyberspace, Journal of the American Academy of Psychiatry and Law 30 (1), 81–94.

McMenamin, J., 2007. Gaumer Convicted of Rape, Murder: Prosecutors Seeking Death Penalty for UMBC Student, Who Met Victim Online, Baltimore *Sun* (May 11).

Meloy, J.R. (Ed.), 1998. The Psychology of Stalking: Clinical and Forensic Perspectives. Academic Press, London, England.

Protect Children from Predators on Internet, Parents Tell Congress. 2000. Psychiatr. News May 5. Available at www.psych.org/pnews/00-05-05/protect.html.

Randazzo, M., Keeney, M., Kowalski, E., Cappelli, D., Moore, A., 2004. Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector. National Threat Center, U.S. Secret Service, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, Washington, DC; Pittsburgh, PA.

Reust, J., 2006a. Case Study: AOL Instant Messenger Trace Evidence. Digital Investigation 3 (4), 238–243.

Reust, J., 2006b. Network Intrusion Investigation: Preparation and Challenges. Digital Investigation 3 (3), 118–126.

Rizzo, T., 2001. Judge Says Robinson Must Stand Trial in Three Deaths. Kansas City Star, March 2. Available at www.kcstar.com/standing/robinson/case.html.

Rogers, M., 1999. The Psychology of Hackers: A New Taxonomy, paper presented at the RSA World Security Conference < San Jose, CA.

Sex, Lies and Murder: *Michigan v. Miller*, 2001. Court TV February 26. Available at www.courttv.com/trials/taped/miller.html.

Shaw, E.D., 2006. The Role of Behavioral Research and Profiling in Malicious Insider Investigations. Digital Investigation 3 (1), 20–31.

Shaw, E.D., Fischer, L., 2005. Ten Tales of Betrayal: An Analysis of Attacks on Corporate Infrastructure by Information Technology Insiders, vol. 1. Defense Personnel Security Research and Education Center, Monterrey, CA.

Shaw, E.D., Post, J.M., Ruby, K.G., 1999. Inside the Mind of the Insider, Business Continuity. Available at www.securitymanagement.com/library/000762.htm.

Shaw, E.D., Ruby, K.G., Post, J.M., 1998. Insider Threats to Critical Information Systems. Technical Report #2; Characteristics of the Vulnerable Critical Information Technology Insider (CITI) Political Psychology Associates. www.pol-psych.com.

Shaw, E.D., Stroz, E., 2004. Warmtouch Software: The IDS of Psychology. In: Parker, T. (Ed.), Adversary Characterization: Auditing the Hacker Mind. Syngress, Rockland, MA, pp. 145–170.

Turvey, B., 2000. Modus Operandi, Motive and Technology. In: Casey, E. (Ed.), Digital Evidence and Computer Crime: Forensic Science Computers and the Internet, second edition. Academic Press, London, England, pp. 147–167.

Washington v. Robert A. Durall, 2003. State of Washington Appellant File Date: 05/05/2003 47928-8-1.