Chapter 13

An Introduction to Cybercriminology: What is Cybercriminology?

Since the first edition of this text was published, the application of criminological theory to the understanding of high-technology/cybercriminals has grown. This emerging field of study, termed *cybercriminology*, is the study of why individuals engage in cyber-related criminal acts such as hacking, identity theft, and digital piracy. Most of the studies thus far have attempted to apply criminological theories developed in relation to physical world crime to the study of cyber-related behaviors. There are several textbooks under development that are devoted to cybercriminology, and there is at least one international journal dedicated to the topic, *The International Journal of Cyber Criminology*.

Thus far, there have been a few historical studies to focus on cybercriminals themselves. In the early days of high-technology crime, there were studies focused on the personality profiles of hackers. On the basis of these studies, it was discovered that hackers were generally very intelligent, maintained very few close friends, and were socially introverted. It makes sense that this was an accurate depiction of a hacker at the time the studies were conducted. Computers at that time were not as widely accepted as they are today, and those who used them were more likely to spend a significant amount of time on them because the devices were not as easy to operate as computers today. Such individuals may have maintained introverted personalities and few friends because they spent so much time on the computer, or possibly spent so much time on the computer because they had few friends. Either way, the individuals involved in the activities were normally of very high intelligence and were very good at computer programming.

However, this is not necessarily the case anymore. Computers are far more popular today, and the technology associated with computers is so much simpler than even 5 or 10 years ago. Today, anyone who is willing to devote just a little bit of time to the topic can develop some basic hacking skills, and even more advanced hacker skills require less training. No

DOI: 10.1016/B978-1-4377-5582-4.00013-3

longer does becoming a hacker require understanding of complex computer technology and programming. Recall the script kiddies discussed in earlier chapters, who are considered by many to be the most dangerous of cybercriminals because they have a limited understanding of how the software programs they use affect a computer system. Due to their ignorance they may do more damage than intended when they launch software programs on target systems. Software programs can now be located with relative ease from websites based around the world. The ease with which an individual can access information on cyber-related crimes today means that it is almost impossible to develop a profile of a computer hacker—or any other high-technology criminal. The person next door with doctorate degrees in physics and computer science is as likely to be responsible for a high-technology crime as the guy next door who dropped out of school in the tenth grade. This means that refining and developing theories associated with cybercrime is more important than ever. [illegible]

In the following section, several criminological theories will be discussed. While developed prior to the focus on high-technology crime, these theories have been applied or tested in relation to several of the cybercrimes discussed in the current text. These theories are Sykes and Matza's techniques of neutralization, Akers's social structure and social learning theory, Cohen and Felson's routine activities theory, Hirschi and Gottfriedson's general theory of crime (sometimes referred to as self-control theory), Becker's labeling theory, and Festinger's deindividuation theory. In addition, one criminological theory was developed in response to the increasing number of cybercrimes encountered today: Jaishankar's space-transition theory.

In breaking with tradition from the previous sections of this textbook, each of the following sections will contain a discussion of criminological theories and then a brief overview of some of the studies conducted in each of the theoretical areas. Because there are a growing number of interesting articles in this area, rather than placing a recommended reading list at the conclusion of the chapter, each section will contain a reading list at the end of the theoretical discussion. These articles are the basis for discussion, and readers are encouraged to seek out these articles in the areas of most interest to them.

Techniques of Neutralization and Rationalization

In 1957, Gresham Sykes and David Matza described their theory of neutralization techniques. These theorists believed that not all juveniles were always opposed to society's values and beliefs, as was a common belief during this time period. The accepted view of juvenile delinquency at the time was that juveniles who engaged in delinquent behavior did so because they adhered to a separate system of values. Sykes and Matza disagreed, arguing that these juveniles could be law-abiding citizens one moment and then engage in delinquent behaviors the next moment. To explain how juveniles could move from law-abiding to criminal, and then often return again to law-abiding, Sykes and Matza proposed five techniques of neutralization used by juveniles to minimize or negate guilt associated with their behaviors. In this manner, a law-abiding juvenile could engage in a delinquent or criminal behavior and then move back to law-abiding in a process of "drift" (as later coined by Matza) by feeling no guilt for their delinquent or criminal behavior. The five initial techniques of neutralization were (1) denial of injury, (2) denial of victim, (3) denial of responsibility, (4) condemnation of the condemners, and (5) appeal to higher loyalties.

Heath Copes, a researcher in the area of neutralization theory, has argued that if one or more of these techniques is employed prior to the commission of the delinquent or criminal act, then the technique is considered to be one of neutralization. However, if the technique is employed after the act is committed, instead of being a technique of neutralization it becomes a technique of rationalization, whereby the offender attempts to rationalize away any guilt associated with the behavior. Three of the techniques are rather self-explanatory in their titles. Denial of the injury is where the offender argues that while someone was victimized by their behavior there was no injury caused during the commission of the act. Denial of the victim, on the other hand, is when the offender argues that while his or her behavior may have technically been wrong, there was no victim of his or her activity and therefore no guilt associated with the behavior. Denial of responsibility is used when the individual argues that something beyond his or her control made him or her engage in the delinquent/criminal behavior. Put simply, the offender may try to argue that someone else made him or her do it.

The final two techniques are slightly more complex. Condemnation of the condemners is used when the individual will attempt to justify his or her behavior on the grounds that the victim of the act is a hypocrite because he or she would engage in similar behaviors if given the opportunity, or perhaps already engages in even worse behavior. Appeal to higher loyalties refers to situations in which an individual will justify his or her behavior on the grounds that while the activity may have violated one or more of society's established values or rules, the act was not necessarily a violation of the values or rules of a subset of society—particularly the offender's friends, gang members, and so on.

In a purely egocentric manner, Sykes and Matza's theory of neutralization and rationalization was selected first because this is the theory this author, along with Elizabeth McMullan, has used to study digital piracy and file sharing. If you remember the earlier discussion on digital piracy, you may remember that the term "digital pirates" refers to individuals who engage in the distribution of copyrighted movies, music, and software files.These individuals do not always attempt to make a profit out of the file-sharing activities and may in many cases be law-abiding citizens in all other aspects of their lives.

The studies discussed in this section are based on university student samples. University students have been used in these studies for a variety of reasons, not the least of which is the fact that students historically have better access to the computers and high-speed Internet connections necessary to engage in file-sharing behaviors. However, it should be noted that these behaviors extend beyond student populations. Anyone who has an interest in music or movies can become a file sharer, as the software is normally very user-friendly and does not take much practice to master. In fact, one time this author was asked to speak about file sharing to a class. While waiting for the host to show up in the division's main office, a conversation ensued between myself and the department secretary.The secretary asked me what I would be talking about, and I informed her that I was there to talk about high-technology crime in general and digital piracy and file sharing in particular. It was only as the digital piracy statement left my lips that I noticed the young lady attempting to minimize the file-sharing program that was running on her office computer. After I assured the woman that I was not there to report anyone for use of file-sharing software, we continued talking and she revealed that a majority of faculty members in the division (9 of 12) downloaded music files on a regular basis. It should be noted that because many universities have now cracked down on the use of file-sharing programs on university-owned computers, this would likely no longer be the case, but the story does show that not just students would occasionally "drift" into behavior that was technically illegal.

In studying file-sharing attitudes, McMullan and I found that a number of individuals indicated support for techniques of denial of injury and denial of victim when engaged in file-sharing behaviors. It was a commonly held belief that downloading music and sharing music and movie files was not harmful to the recording artists because they still got their money from concerts or from the recording companies. Some of the individuals even claimed that they would use downloading and file sharing to help them select which CDs to purchase. However, in an ironic twist, these same individuals would later claim to have purchased very few CDs over the 12-month period before our interview. Yet others indicated support for techniques of neutralization and rationalization developed after Sykes and Matza released the original version of their theory. For example, one of the individuals we interviewed actually stated that he was "entitled" to download and share files because he paid a flat rate for Internet service. The individual felt that as such he was entitled to anything that he could obtain with that Internet connection.

While our study was more qualitative in nature, Sameer Hinduja, a known researcher and author in the areas of cybercrime and cyberbullying, has conducted at least one quantitative study on neutralization and digital piracy. Hinduja surveyed slightly more than 400 university students and found neutralization techniques to be weakly related to file sharing. However, Hinduja's study focused on attitudes of file sharing in regard to software piracy. As Hinduja noted in his research, many of the individuals did not appear to consider software piracy to be a moral issue. Hinduja noted that the future of regulating software piracy would possibly lie in developing a better moral understanding of digital piracy among file sharers.

George Higgins, another criminologist who has published extensively on cybercriminology, along with colleagues Scott Wolfe and Catherine Marcum, conducted a short-term longitudinal study on music piracy and neutralization techniques. Over the course of four weeks, approximately 200 students were surveyed concerning the file sharing of music files and the use of neutralization techniques by file sharers. Higgins and his colleagues discovered that digital piracy could be related to neutralization techniques. Interestingly, these researchers also found that as the study progressed, respondents in the study indicated lower levels of file sharing. As noted by the researchers, this could possibly be explained by the fact that participants may have begun to reevaluate their behaviors on a regular basis because of their participation in the study. In reflecting on their file-sharing behaviors, some participants may have come to believe that file sharing was inappropriate behavior. Each of the above researchers has noted that digital piracy is a growing area of criminological research, and there is a need for further study in the area of file sharing in general and neutralization techniques specifically.

Further Reading

Higgins, G., Wolfe, S., & Marcum, C. (2008). Music Piracy and Neutralization: A Preliminary Trajectory Analysis from Short-Term Longitudinal Data. *International Journal of Cyber Criminology*, 2(2), 324-36.

Hinjuda, S. (2007). Neutralization Theory and Online Software Piracy: An Empirical Analysis. *Ethics and Information Technology*, 9, 187-204.

Moore, R. & McMullan, E. (2010). Neutralizations and Rationalizations of Digital Piracy: A Qualitative Analysis of University Students. *International Journal of Cyber Criminology*, 3(1), 441-51.

Social Structure and Social Learning Theory

Social structure and social learning theory are the work of Ronald Akers. Akers agreed with an earlier criminologist, Edwin Sutherland, who developed what is known as differential association theory. Akers, however, disagreed with some aspects of differential association. As a result, he felt that Sutherland's theory was incomplete. Sutherland had proposed the idea that criminal or delinquent behaviors were learned from individuals, but the belief was that the specific mechanisms that aided learning were never fully addressed in previous works. Akers relied heavily upon behavioral science in reaching these conclusions. Ultimately it was Akers's determination that individuals are more likely to engage in criminal behavior when they frequently associate with people who not only engage in criminal behavior but also teach an attitude of acceptance for criminal behavior.

One of the more interesting expansions that Akers made on Sutherland's differential association was the belief that individuals could in fact learn criminal attitudes and behaviors (to include behaviors and the actual techniques of criminal behavior) through the media and other forms of nontraditional communications. The most important associations are those that occur on a regular basis and involve encounters with those who are closest to the individual (e.g., family, close personal friends, etc.), but with Akers's contention that nontraditional communications could provide a forum for communicating definitions and ideas favorable to committing delinquent acts, the door has been opened for studies involving the role of online relationships, websites, and virtual communities in the learning of delinquent attitudes.

If relationships can explain why some individuals develop an affinity for committing delinquent and criminal acts, then online relationships should be further examined. There are literally thousands of websites where people can "meet" and chat about their interests, their hobbies, and even their love lives. It is not unfathomable that an individual who is devoted to this form of electronic communication could become involved enough in the community that the social learning process Akers advocated could develop. Some individuals devote hours every week to chatting and responding to online discussion forums and virtual communities. If these websites and discussion forums are devoted to activities such as identity theft or the distribution of digital child pornography, then it is possible that someone could learn from these "virtual" communities. A web-based community devoted to cyber-related deviance could convey not only the techniques related to cybercrime but also the beliefs that such behaviors are acceptable, justifiable, or even necessary in today's society.

A study examining this phenomenon was conducted by faculty members from Drexel University. Rob D'Ovidio, Tyson Mitman, Imaani Jamillah El-Burki, and Wesley Shumar examined a series of websites that advocated or supported sexual relationships between adults and children. These researchers located approximately 64 websites that advocated such relationships and then examined these websites for the presence of electronic communication tools that could be used in conveying definitions favorable to sexual relationships between children and adults, as well as those that would allow for the teaching of techniques to be imitated by others.

The results of their study revealed that one-fifth of the websites they examined maintained instant messaging or synchronous chat for users, while more than half (approximately 57.8%) provided a discussion forum where members could post stories, questions, comments, and so on.

Even more interesting were the findings that more than 60 percent of the websites contained content that conveyed neutralization techniques such as condemnation of the condemners and denial of injury.These techniques, in conjunction with other discussion board forums, could in fact be used to communicate definitions favorable to violation of the laws related to sexual relationships between children and adults.This is a key component of both Sutherland's differential association and Akers's social learning theory. On the basis of these results, D'Ovidio and colleagues argued that virtual communities built around such websites could in fact become places of social learning. One very interesting recommendation to come from this research was the argument that probationers and parolees of crimes related to sexual offenses against minors should have their probation and parole conditions adjusted to reflect the potential criminal nature of such websites. Put simply, these researchers argued that courts should restrict access to such websites as a condition of their probation and parole. Some states have begun limiting Internet access of sex offenders, although such restrictions can be difficult to monitor.

George Higgins and David Matkin surveyed approximately 318 university students concerning software piracy, in an attempt to measure the impact of social learning on self-control (to be discussed later in this chapter). The results of their study revealed that social learning theory is important in understanding why individuals engage in software piracy. More specifically these researchers found that having friends who engage in software piracy was influential in determining whether someone would engage in software piracy.These findings, as noted by the researchers, are consistent with other studies that have found that having friends who engage in, and likely encourage participation in, a particular activity will influence a person's desire and willingness to engage in a deviant or criminal activity.With this in mind, Higgins and Makin recommended that future education and awareness programs dealing with software piracy should focus on making peers more aware of the legal and procedural dangers associated with software piracy.

Further Reading

D'Ovidio, R., Mitman, T., El-Burki, I., & Shumar, W. (2010). Adult-Child Sex Advocacy Websites as Social Learning Environments: A Content Analysis. *International Journal of Cyber Criminology*, 3(1), 421-40.

Higgins, G. & Makin, D. (2004). Does Social Learning Theory Condition the Effects of Low Self-Control on College Students' Software Piracy? *Journal of Economic Crime Management*, 2(2), 1-22.

Routine Activities Theory

Lawrence Cohen and Marcus Felson approached the study of criminal behavior from a different perspective than the previous theorists. These criminologists accepted that criminal behavior and the criminal attitude are rational choices. Instead of focusing on the individual directly, these theorists focused on how activity patterns can affect crime rates and victimization. According to Cohen and Felson, there are three factors that must be considered when examining crime: (1) the presence of a motivated offender, (2) a suitable target for victimization, and (3) an absence of capable guardians to prevent victimization. Examining the crime of burglary can help to further explain this theory. An individual who is interested in burglarizing a residence is more likely to break into a home where he or she feels he or she has the best opportunity to successfully complete the activity. In a nicer, more affluent neighborhood, it may be more likely that neighbors will take care of each other's property when the residents are away from home. Therefore, there is a greater likelihood that someone would report suspicious behavior in or around the residence. Further, there is the possibility that the homes in these nicer neighborhoods will contain high-tech alarm devices that alert law enforcement to any unlawful entry into the residence.

However, what if this potential burglar were to consider breaking into a residence in a poorer neighborhood? Perhaps in this neighborhood the residents have to work two jobs in order to make ends meet. In this neighborhood, the factors for criminal behavior are much better. First, we have a motivated offender, a potential burglar who wants to commit the crime of burglary and wants to succeed at his endeavor. Second, there is a suitable target, a residence containing property that could be stolen and then quickly resold to make some quick and easy money. Finally, there is an absence of capable guardians; that is, the residents work away from the home and therefore will not be home to prevent the burglary. Unlike in the upper-class residence, there is also less chance of a working alarm system being in place inside the residence. As a result, the situations in the second neighborhood are more conducive to the commission of the act of burglary.

In describing their theory, called *routine activities theory* (RAT), Cohen and Felson noted property crime rates over several decades and argued that increased numbers of property crimes could be attributed to the fact that more women were entering the workforce and therefore leaving the residences unguarded during the day. There are several high-technology crimes that could be potentially studied through the lens of routine activities theory, such as hacking. On the Internet, motivated offenders can more easily find potential targets and then victimize the users if their computers do not contain capable guardians (i.e., anti-virus software or working firewalls).

Adam Bossler and Thomas Holt conducted a study of approximately 500 university students in an attempt to determine the applicability of routine activities theory to a user's computer becoming infected with malware. Bossler and Holt found that physical guardianship and ensuring that a user's computer maintained up-to-date anti-virus software was not related to victimization. However, individuals who engaged in digital piracy or had friends who viewed pornography on the Internet were more likely to experience malware. As these researchers noted in their conclusions, these areas of Internet use (pornography and digital piracy) are excellent opportunities for motivated offenders to seek out potential targets—given that both are very popular among younger age groups. However, Bossler and Holt admitted that while their study provided some initial support for applying the theory to computer-related victimization, there was still a need for further studies to fully understand the theory's usefulness in this area. Kyungshick Choi conducted a similar study, using approximately 200 university students. Choi found that online behaviors were related to routine activities theory in his study, but he noted that the guardianship factor (i.e., anti-spyware, anti-virus, etc.) was related as well. According to Choi, having these software programs would lower computer crime victimization.

As these studies show, there is some general support for the use of routine activities theory as a means of better understanding online victimization. All of the above studies agree that routine activities theory has its place in the field of cybercriminology. The only study to directly argue against the use of routine activities theory was written by Majid Yar, whose ideas are discussed by Holt and Bossler in their article on applying lifestyle routine activities theory to cybercrime victimization. Yar's research states that cybercrime is a new form of crime for which past theories may not be applicable. Specifically, Yar argues that many of the components of routine activities theory appear applicable to the study of online victimization, but there remain significant differences between the crimes that occur in what Yar refers to as "virtual" worlds versus that of the "terrestrial" world. There is definitely a need for further study, particularly as the issue of a capable guardian has not been clearly addressed.

Further Reading

Bossler, A. & Holt, T. (2010). Online Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, 3(1), 400-20.

Choi, K. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, 2(1), 300-33.

Yar, M. (2005). The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, 2(4), 407-27.

Self-Control Theory—General Theory of Crime

Michael Gottfriedson and Travis Hirschi developed a general theory of crime in 1990 that would come to be referred to as *self-control theory*. According to this theory, there are several elements of self-control that relate to criminal behavior.The first is that criminal acts provide immediate gratification. Individuals who suffer from low self-control may have trouble deferring gratification and will engage in behaviors that provide short-term pleasure even if the activities could lead to long-term harm. Some criminal acts, for example, are believed to provide money in exchange for little work (e.g., theft or robbery).The second element is that criminal activities are exciting or thrilling. Individuals who have problems with low self-control may find that criminal activities involving stealth and the risk of getting caught are exciting. Higher levels of self-control might make one more cautious and less likely to engage in criminal behavior.The third element is that criminal behavior provides few long-term benefits. This means that the activities are not equivalent to an actual career and, while the activities are exciting for a short period of time, they ultimately provide little or nothing.The fourth element is that crime requires little skill or planning. This means that individuals who engage in most crimes do not have to preplan the activities and do not have to maintain advanced skills to engage in the behavior.That is, when an opportunity to engage in criminal behavior is presented, the person with low self-control may be more likely to engage in the criminal behavior. Gottfriedson and Hirschi felt that these behaviors could be attributed to a lack of effective parenting.Thus, parents who failed to form an early attachment to their children would eventually fail to monitor the behavior of their children. Over a period of time these children would then develop the aforementioned issues and would have problems controlling their tempers, as well as their behaviors.

George Higgins examined self-control theory as it relates to understanding digital piracy on a university sample. Surveying approximately 382 students, Higgins examined the relationship between self-control levels and intentions to engage in digital piracy. Using a measure of self-control validated in several previous studies, Higgins found that low levels of self-control did in fact have both direct and indirect effects on respondents' intentions to engage in digital piracy. Higgins noted that these results show that changing the focus of anti-piracy campaigns to include shaming or increased understanding of the moral issues associated with digital piracy could be a means of regulating the behaviors.

Self-control appears to be a valid theory to examine in light of several high-technology crimes. Individuals with lower levels of self-control may be more inclined to engage in other cyber-related deviance as the techniques associated with such behaviors become increasingly easier to master.This is a valid concern given that many software programs are currently being released on Internet websites that allow users with less technical skill to engage in more technical cyber-related activities. Understanding the role of self-control on cybercrime activities is sure to become an even greater researched area in the near future.

Further Reading

Higgins, G. (2007). Digital Piracy, Self-Control Theory, and Rational Choice: An Examination of the Role of Value. *International Journal of Cyber Criminology*, 1(1), 33-55.

Labeling Theory

Frank Tannenbaum provided the foundation for labeling theory in 1938 when he discussed his belief in "the dramatization of evil." With this theory Tannenbaum was arguing that anytime a person's behavior causes them to be singled out in a negative manner, then that person will begin to define him- or herself in light of these beliefs. Put simply, a person will become the monster that their behavior has led them to become known by. While Tannenbaum is perhaps the founder of labeling theory, Howard Becker is perhaps the best known labeling theorist. Becker redefined labeling theory when he discussed the concept of the "moral entrepreneur." According to Becker, moral entrepreneurs are individuals who seek to criminalize certain behaviors on the basis of moral beliefs.

As a result of certain behaviors being criminalized, a person who may not have a moral objection to the behavior but is caught engaging in the behavior becomes known as a criminal. This label of criminal can become the identity by which an individual may come to identify himself. Over time the individual who has obtained the label of "criminal" may come to view him- or herself as a criminal. Perhaps this acceptance of the label is the result of having the term reinforced by their social peers or perhaps just resigning him- or herself to the label given them by society. Once people perceive themselves as criminal, they may be more likely to give up trying to abide by the rules of society and may instead focus on living up to the deviant/criminal label. As a result, future behaviors may be geared toward developing and enhancing recognition as the type of person they have been labeled. For example, the individual who has been called a violent criminal may over time engage in progressively more aggressive violent behavior.

There have been few studies to examine labeling theory in light of high-technology crimes. Orly Turgeman-Goldschmidt, an Israeli criminologist, conducted one such study on the meaning that hackers can assign to their label as a hacker. Turgeman-Goldschmidt conducted in-depth interviews with approximately 50 self-defined hackers in Israel. Turgeman-Goldschmidt noted that the definition of hacker has changed in recent decades. If you reflect back to the discussion on the history of hacking in Chapter 2, you will recall that hackers were historically individuals who were very skilled in computer programming and capable of making computer programs do more than they were originally intended to do. Over time, however, the term has come to refer to individuals who engage in criminal behaviors that involve the use of computer-related technology in the commission of the crime, that is, breaking into a computer system and causing harm to the computer system.

Turgeman-Goldschmidt noted that because the term *hacker* has come to be associated with computer-related criminal behavior, some individuals who engage in computer-related activities may earn the label of hacker and begin to respond to it. The researcher noted the possibility that these individuals may view themselves as different from "mainstream" computer users and adapt accordingly. Turgeman-Goldschmidt found that one individual he interviewed focused on the fact that as a hacker he was expected to fit a certain profile, and claimed that he was unsuccessful at many things in life. Despite this, Turgeman-Goldschmidt found that this particular hacker had in fact completed many successful mainstream achievements, not the least of which was a tour of duty in the military as an officer.

Interestingly, when examining the "master status" of these hackers, Turgeman-Goldschmidt found that hackers in his study seemed to indicate support for the status of "computer expert" rather than "computer deviant." These individuals do not suffer from a lowered value for themselves or their self-identity, but on the contrary seek out the label of "hacker" because it makes them feel more accomplished. Of specific interest to Turgeman-Goldschmidt was the fact that unlike other deviant labels, the label "hacker" did not appear to negatively influence employment potential. If anything, the results of the study indicated that self-defined hackers were financially successful and had little trouble finding employment. As Turgeman-Goldschmidt noted, these findings are different from what one would expect, and they provide support for the belief that more research in this area could help criminologists better understand how labeling related to high technology–related deviance differs in relation to labeling as the theory relates to non-cybercrime deviance.

Further Reading

Turgeman-Goldschmidt, O. (2008). Meanings That Hackers Assign to Their Being a Hacker. *International Journal of Cyber Criminology*, 2(2), 382-96.

Deindividuation Theory

In 1952, Leon Festinger, Albert Pepitone, and Theodore Newcomb released their theory of *deindividuation*. According to these social psychologists, individuals who engage in group-related activities may lose their self-identity and become a part of the group. Without the sense of self to regulate one's behavior, the person may become more uninhibited and begin engaging in deviant or criminal behavior. The foundation for this theory is believed to have begun with Gustave Le Bon's work on crowd behaviors (e.g., lynch mobs, Mardi Gras revelers, etc.). After a person loses his or her self-identity, he or she may be more likely to engage in behaviors that go against his or her personal beliefs and fall more in line with the beliefs of the group. One of the more interesting studies to be linked to deindividuation theory is that of the Stanford prison experiment, whereby students were divided into prisoners and correctional officer groups. During the course of the study, researchers found that the students portraying correctional officers began to use excessive force on the students portraying prisoners. Deindividuation has been argued as an explanation for why the students portraying correctional officers became more aggressive in a situation in which their identity was concealed. Additionally, both groups of students were dressed and identified in such a manner that the individuality of the students was removed during the course of the study (which, incidentally, ended after only six days because of concerns for the safety of the students portraying inmates). Readers who are interested in learning more about this study and deindividuation are encouraged to read Philip Zimbardo's *The Lucifer Effect*, which was written by the principal investigator of the Stanford prison experiment.

There has been an increase in interest concerning deindividuation theory as it relates to Internet behaviors. Given the perceived anonymity of the Internet, it has been argued that deindividuation on the Internet could lead individuals to engage in behaviors that they normally would not engage in. Christina Demetriou and Andrew Silke of the University of Leicester conducted an interesting study involving the Internet and deindividuation. Demetriou and Silke established a fake website that was touted as a source for shareware, freeware games, and software applications. Over the course of 88 days the researchers recorded the browsing habits of the 800 individuals who accessed the website. The researchers found that the vast majority (all but approximately 58) of individuals accessed the website looking for legal materials. However, the authors had established a number of website links that pointed to illegal or deviant materials—the illegal materials being pirated software or video game links and the deviant materials being hardcore pornography. It should be noted that because of the illegal nature of some of these links, the links were inactive, and users who selected the links were taken to blank pages.

The researchers indicated that they were interested in seeing how many people would access the website for a legitimate reason (access freeware or shareware games and apps) and would then engage in deviant or criminal behavior because the links were available to them. Their findings were interesting in that 81 percent of the individuals who visited the website for legal games and software attempted to access the illegally hacked games page. Out of 297 individuals who accessed a fake webpage containing supposed hacked passwords to paid-only pornographic websites, 289 of these individuals accessed the page after arriving at the website for legitimate purposes. These researchers stated a belief that deindividuation may impact an Internet user's behavior when he or she believes he or she is anonymous on the Internet. However, it is worth noting that this study could not confirm anonymity as a cause for individuals selecting the illegal websites. The researchers note that it is possible that individuals who visited the website may have accessed the materials without realizing that they were doing so. Nevertheless, this study is an interesting look at deindividuation, anonymity, and Internet behavior from a nontraditional approach.

Sameer Hinduja examined software piracy through the lens of deindividuation in a university student sample. In surveying more than 500 university students, Hinduja asked respondents to answer a series of questions designed to measure their opinion of anonymity and pseudonymity. These questions asked respondents, "The anonymous nature of the Internet is something that I value" (anonymity measure), and "Individuals should be able to assume different identities, personas, and roles while using the Internet if they so choose" (pseudonymity measure). With this study, Hinduja was testing whether the anonymity of the Internet would allow an individual to develop group values and beliefs about digital piracy, thereby losing his or her individual personality and affecting his or her frequency of engaging in digital piracy. What Hinduja found was that there was no statistically significant increase in respondents' participation in digital piracy when examining anonymity and pseudonymity. Hinduja noted that these results were in contradiction to past studies on deindividuation. However, Hinduja also noted that the isolation of an individual could contribute to an individual's deviant behavior because these individuals do not have the same social controls that come from being a part of a group. As such, an individual who engages in deviant behavior via the Internet may do so because he or she has no social group to regulate his or her behaviors.

Both of the above studies provide a foundation for a significant area of future study: the role of anonymity in Internet-based deviance and criminality. Deindividuation theory argues that individuals become a part of a group, and as a member of the group they lose their individuality. The studies that have examined deindividuation in the virtual world, however, have had mixed results. What are some possible explanations? Perhaps Hinduja was onto something when he stated that an individual's Internet behaviors are often the result of individual and isolated behavior. Few individuals, outside of some groups of online video gamers, get together and browse the Internet in groups. As such there is something to be said about the role of isolation and anonymity. Deindividuation is certainly a valid theory, and one that does appear to support "mob mentalities." However, much as Yar argued in relation to routine activities theory, it is difficult to apply a terrestrial theory to a virtual activity.

Anonymity on the Internet does likely impact an individual's behaviors. Based on academic interviews conducted by this author, as well as anecdotal discussions with individuals arrested for stalking and harassment via electronic means (a misdemeanor in several states), there may be more to anonymity than a mere relaxation of belief. In fact, some of the individuals noted in our discussions that they would find themselves engaging in behaviors, and though they believed they were wrong, they felt like it was okay. This is not to say that they felt that the anonymity caused the criminal behavior. Rather, these individuals felt that the anonymity of the Internet allowed them to go further than they would have had they been face-to-face with the person they were harassing. These individuals repeatedly made the claim that they never would have done or said some of the things they said or did had they been face-to-face with their victims. Therefore, could it be that the anonymity of the Internet acts to enhance a person's behavior—perhaps enhancing the level of activity to the point at which the person engages in criminal behavior beyond what they normally would because they (1) feel they are less likely to be identified (many of the individuals arrested did not realize that e-mails and text messages sent via computer could be traced), and (2) do not have to witness the impact their behaviors have on victims. Perhaps people gradually increase their level of deviant behavior over time because of a lack of restrictions placed on them by a social group, as Hinduja argued.

This anonymity-enhancement argument could potentially explain why individuals who engage in digital piracy repeatedly have stated to this author that they have never even considered shoplifting a music CD or a video DVD—even though these same individuals recognize that the behaviors are very similar. Again, this information needs to be further examined through future studies that focus on anonymity and whether it can enhance a person's behavior to the point of explaining their participation in some cyber-related deviance. Certainly past studies such as the ones discussed have shown that anonymity may play a role in a person's decision to engage in cyber-related behavior. Other studies have hinted at the fact that anonymity could potentially explain certain online behaviors.

Further Reading

Demetriou, C. & Silke, A. (2003). A Criminological Internet "Sting." *The British Journal of Criminology*, 43(1), 213-22.

Hinduja, S. (2008). Deindividuation and Internet Software Piracy. *CyberPsychology & Behavior*, 11(4), 391-8.

Space Transition Theory

Each of the previously discussed theories was a theory developed in relation to physical-world crime. This final theory was developed as a response to a need to begin developing theories that address crimes in the virtual world. K. Jaishankar, a criminologist who specializes in cybercriminology, has proposed a theory that is specifically formulated for crime that occurs through use of the Internet. This theory argues that people can behave differently depending on whether they are engaged in behaviors in the "physical space" versus when they are engaged in behaviors in the "cyberspace."This theory has been termed *space transition theory* and is composed of seven propositions that attempt to explain deviant/criminal cyber-related behaviors. These propositions are:

> *Persons with repressed criminal behavior (in the physical space) have a propensity to commit crime in cyberspace, which, otherwise they would not commit in physical space, due to their status and position.*—This proposition argues that some people do not commit crime in physical space because they fear being caught and losing their social status through sanctioning or embarrassment. However, in cyberspace these individuals may perceive that their chances of being stigmatized or sanctioned are less because there is no one around when the cyber-related criminal acts occur. These individuals may engage in criminal behavior at greater rates.
>
> *Identity flexibility, dissociative anonymity, and lack of deterrence factor in the cyberspace provide the offenders the choice to commit cybercrime.*—The proposition here is that individuals who engage in cyberspace crimes are able to take advantage of the anonymity factor associated with online identities. Individuals may convince themselves that they cannot be identified and therefore may engage in behaviors that they normally would not. Moreover, some activities may not be criminalized in all areas of the world; therefore, there is little deterrence for engaging in online criminal behaviors.
>
> *Criminal behavior of offenders in cyberspace is likely to be imported to physical space, which, in physical space, may be exported to cyberspace as well.*—This proposition argues

> that cybercrime is becoming more attractive to traditionally physical-space crime groups (organized crime groups, etc.), and traditional cybercriminals are being replaced by modern physical-space criminals who are now taking advantage of the fact that law enforcement agencies may have trouble tracking the activities of criminal activity in cyberspace.
>
> *The intermittent venture of offenders in cyberspace and the dynamic spatiotemporal nature of cyberspace provide the chance to escape.*—According to this proposition, cybercriminals enter and leave cyberspace much as physical-space criminals would enter and exit a crime scene. However, in the case of cybercrimes the activities can occur from all over the world and allow for the commission of advanced crimes in less time.
>
> *(a) Strangers are likely to unite together in cyberspace to commit crime in the physical space; and (b) associates of physical space are likely to unite to commit crime in cyberspace.*—This proposition argues that the vast number of websites, discussion forums, and chat rooms provides an increased number of recruitment opportunities whereby individuals can easily post information related to criminal attitudes and techniques.
>
> *Persons from closed society are more likely to commit crimes in cyberspace than persons from open society.*—According to this proposition, individuals who come from closed societies may not have the ability to convey their beliefs and thoughts publicly. Therefore, these individuals may resort to such expression in cyberspace, and may then engage in a variety of cyber-related deviance and criminal behavior.
>
> *The conflict of norms and values of physical space with the norms and values of cyberspace may lead to cybercrimes.*—This proposition states that cybercrime could be the result of conflicts between the norms of individuals who may come from a variety of places around the world. Further, because some groups in cyberspace have begun developing norms related to online behavior, it is possible that a person in cyberspace may find him- or herself engaged in delinquent or criminal behavior as a result of a conflict between that person's norms and the norms of others from around the physical space and cyberspace.

In examining the propositions above, several components of the space transition theory appear to be valid explanations of cyber-related criminal behavior. It should be noted that while some of the propositions could also potentially be used to explain physical crimes, Jaishankar points out that his theory is only an explanation for cyberspace crime and not physical-space crime. The theory contains many aspects of previously discussed theories, as well as a few new ideas as they relate to cyber-related behaviors. It will be interesting to see how this theory tests empirically, but the mere development of the theory is something for which Jaishankar should be commended. Over the next several years there will likely be additional theories proposed, as cybercriminology becomes a more recognized specialization in the fields of criminal justice and criminology.

Further Reading

Jaishankar, K. (2009). Space Transition Theory of Cyber Crimes. In Schmalleger, F. & Pittaro, M. (eds.), *Crimes of the Internet*. Upper Saddle River, NJ: Prentice Hall.

Conclusion

Many of the theories thus far examined by cybercriminologists have been based on theories developed in the past for physical-world crimes. Such approaches to understanding cybercrime have been relatively successful, with moderate support being found for theories such as techniques of neutralization, self-control theory, and routine activities theory, among others.

Neutralization techniques, as proposed by Sykes and Matza, have been found in studies focusing on hackers and digital file sharers. These individuals have been found to use denial-of-injury and denial-of-victim techniques to minimize any guilt associated with their behaviors. These techniques allow otherwise law-abiding individuals to engage in cyber-related deviance without feeling guilt related to their behavior. Likewise, studies on self-control theory have found that individuals with lower levels of self-control tend to be less able to resist the urge to engage in digital piracy. Even though there are potential consequences of such behavior, individuals who engage in digital piracy tend to prefer the immediate gratification of file sharing (instant and free music, movies, etc.). Routine activities theory, while finding support among some researchers, is ripe for further study. Online behaviors have been shown to be related to increased likelihood of encountering potential offenders, and the greater numbers of individuals who are online at any given time has increased the number of potential targets. However, the various studies have found different results in terms of whether the presence of a capable guardian (anti-spyware and anti-virus programs, etc.) reduces the likelihood of victimization.

Perhaps the most interesting developments in this area of criminology have been the movements to develop new and innovative theories that attempt to explain crime that is specific to cyberspace. Space transition theory, while still in early stages of development, appears to attempt to do just that. This new theory appears to contain several propositions that would seem to explain certain cyber-related behaviors, and the theory will likely be empirically tested in the future. There is no denying that this area of criminology is extremely exciting and certain to become a well-researched area of criminal behavior.

Review Questions

1. Do you think that it is important to gain a better understanding of theories associated with why individuals may engage in criminal behavior? Why or why not?

2. What is self-control theory? Beyond the criminal behaviors discussed in this chapter, can you think of any cybercrimes that might be explained by this theory?

3. Techniques of neutralization have been found in past studies on digital piracy. How do these techniques work to further criminal behavior among digital pirates?

4. According to research by Hinduja, how does the concept of anonymity impact a person's behavior while on the Internet? Do you agree or disagree with these findings, and why?

5. Do you believe that anonymity can cause individuals to behave more aggressively than they would if they knew they were identifiable or talking with someone face-to-face? Why or why not?

6. What propositions of space transition theory do you feel are the best explanations for deviant cyber-related behaviors?

7. Which propositions of space transition theory do you feel are the least likely to explain such behaviors?

8. Discuss the theory of labeling as it relates to a person becoming labeled a "hacker." How does this label affect that person's future behavior?

9. What are some of the difficulties associated with applying criminological theories developed for crimes in the physical space to crimes in the cyberspace?

10. Are there any criminological theories not discussed that you believe could be adapted to address high-technology crimes? What are these theories, and why do you feel the theory (or theories) would be applicable?

Online Resources

The American Society of Criminology—Home of the American Society of Criminology, which is dedicated to fostering international discussions on criminological theory. Contains a variety of links related to studies and information on various criminological theories as well as news updates. Available at www.asc41.com.