1

Crime Online: Correlates, Causes, and Context

Thomas J. Holt

In 2009, Heartland Payment Systems announced that their system security had been compromised during 2008 by a small group of hackers. The company processes over 11 million credit and debit card transactions for over 250,000 businesses across the US. The impact of the breach was massive, as hackers were able to acquire information from 130 million credit and debit cards processed by 100,000 businesses (Verini 2010). This was the largest breach of customer data in the United States and was thought to stem from malicious software planted inside of the company's network in order to record payment data sent from retail clients (Krebs 2011). Even more disconcerting, this breach was apparently masterminded by Albert Gonzales and a few other hackers who compromised the payment systems of Marshall's department stores and its parent company, TJX, a few years prior. That compromise led to the loss of 45 million credit card records and over $1 billion dollars in customer damages (Roberts 2007). Thus, these actors were not simply hackers who were lucky enough to make one big score. Instead, they were proficient and dedicated repeat offenders who sought out high value targets in succession and made lucrative profits as a result.

Data breaches continue to be a problem, particularly in the United States where millions of customers' data have been lost. Several major retailers in the US experienced breaches leading to the loss of millions of customer data in 2013 and 2014, including Target, Home Depot, Neiman Marcus, and various restaurant chains including Dairy Queen, Jimmy John's, and P. F. Chang's (Higgins 2014; Pauli 2014; Seals 2014). In fact, some referred to 2014 as the "year of the data breach" due to the large number of incidents. These incidents are not limited to retailers, as the health insurance provider Anthem Health Care was compromised by hackers in 2014 and 2015. The actors were able to acquire personal information on as many as 80 million Americans, including names,

dates of birth, social security numbers, addresses, employer information, and income (Abelson and Creswell 2015).

These incidents serve as key examples of the problem of crime stemming from the use of computer technology and the Internet. News reports have increased worldwide regarding the tremendous impact of computer attacks against businesses and personal web users alike (Furnell 2002; Taylor, Fritsch, Liederbach, and Holt 2010). Press coverage of viruses and malicious software indicate the risks that many computer users face from computer based attacks (Brenner 2008; Wall 2007). There is also growing evidence that technology is being used to facilitate social protests against governments on and offline, as evident in the recent Arab Spring (Stepanova 2011) and cyber attacks by the group Anonymous (Denning 2011). The totality of these issues emphasizes the need to understand how modern society can cope with the threats posed by the ubiquity of technology.

In fact, access to computers and high-speed Internet connectivity have dramatically changed the way people communicate and do business around the world, with far reaching consequences that affect all facets of modern life (Jewkes and Sharpe 2003). Most every critical financial, government, medical, business, and private entity is connected through the global interconnected computer networks which constitute the Internet. As a result, a massive amount of information and resources can be leveraged to benefit consumers and citizens. Businesses depend on the Internet to draw in commerce and make information available on demand. The banking and financial industries have implemented new technology enabling customers to gain electronic access to their funds and manage accounts.

The ability to utilize these resources is derived directly from low-cost, easy-to-use home computers coupled with home-based, high-speed, dedicated Internet access. In fact, there are now 3.079 billion Internet users worldwide, with over 1.4 billion users in Asia compared to 310 million in North America (Internet World Stats 2015). Individuals between the ages of 18 and 34 now own the most technological resources and are among the heaviest Internet users in the United States (Lenhart, Purcell, Smith, and Zickuhr 2010). There are approximately 18 million youth online every day using CMCs in various ways. For instance, 89 percent of youth send or read email while online, and 81 percent play online games (Lenhart et al. 2010). In addition, individuals between the ages of 18 and 34 comprise 49 percent of the entire population of Facebook users in the United States (socialbakers 2011).

Smart phones and tablet PCs allow users to be connected to the Internet at all times to do everything from check email to regularly update social networking profiles. Over 80 percent of adults own a cell phone, and almost one

third of those are smart phones that can be used to check their email or connect to the Internet (Smith 2011). Today, youth acquire their first cell phones when they are between the ages of 12 and 13 (Lenhart 2010).

Though the growth and penetration of computer technology has many benefits, it has also spawned a range of deviant and criminal behaviors with unique challenges to law enforcement and the legal system (Wall 1998, 2001; Yar 2005). As noted in the mass compromises discussed earlier, the prevalence of networked computers and databases enables individuals to come into contact with a massive number of potential victims with little effort. In fact, one of the common forms of fraud perpetrated online is Nigerian email schemes, where individuals claim to be foreign princes or bankers who need assistance in moving large sums of money (Holt and Graves 2007; Newman and Clarke 2003; Wall 2004). They request information from the email recipients so that they can reuse the information for identity theft or bank fraud. Criminals can send out millions of emails in a short amount of time to identify and solicit potential victims for fraud schemes (Grabosky et al. 2001; Holt and Graves 2007; Newman and Clarke 2003). By casting a wide net of email messages, the offenders increase the likelihood of finding a victim that will respond (Buchanan and Grant 2001; Wall 2004). Thus, email and other computer-mediated communication methods are ideal for fraudsters because even if a small percentage of individuals respond, they can still obtain a significant amount of money or information (see Holt and Graves 2007; Newman and Clarke 2003).

Virtual environments are also an ideal mechanism for attacks against nation states and large groups due the ability to effectively compromise a target with minimal physical engagement and conceal the origin of the attack (Brenner 2008; Denning 2001). An excellent example of such an attack in action is that of Stuxnet, a computer worm that was used in attacks against the Natanz uranium enrichment facilities in Iran (Clayton 2010; Kerr, Rollins, and Theohary 2010). This malicious software was designed to specifically compromise and harm computer systems called Programmable Logic Controllers (PLCs) inside of centrifuges in these plants in order to surreptitiously but systematically hinder the development of the Iranian nuclear program (Clayton 2010; Kerr et al. 2010). Recent evidence suggests that this program was created by the United States under the Bush administration and actively implemented by an executive order of President Obama because it was thought that this sort of attack would be more targeted, difficult to detect, and produce fewer civilian casualties or collateral damage than a physical strike (Sanger 2012). As a result, cyber-attacks may be an increasingly common way for nation-states to engage one another to cause harm.

In addition, computer technology affords criminals a significant degree of anonymity. Individuals can create fictitious user profiles to hide their real identities, as with hackers who create screen names or "handles" that protect their actual identity while engaging in hacking (Jordan and Taylor 1998, 765). Similarly, individuals can use a variety of technology to mask their physical location. For example, individuals who pirate music and media often utilize a technology called "torrents" as a means of reducing their likelihood of detection (see Holt and Copes 2010). Torrent programs enable individuals to download bits of a larger file, such as a complete album or discography for a musical group or motion picture, from multiple computers, making it difficult to trace the original location of where the file was found or who actually maintains the media (Holt and Copes 2010).

In light of the significant threat posed by computer and cybercrimes, there is a strong need to identify and understand the nature of online criminality, as well as the causes and correlates of cybercrime. Thus, this chapter will provide an overview of computer and cybercrimes, including the complexities of defining these problems and measuring the prevalence and incidence of offenses. A framework to understand and examine cybercrime is also discussed in detail to give some insight into the diverse threats online. Finally, the chapter concludes by outlining the chapters of this book and their contribution.

Defining and Measuring Cybercrime

In order to understand cybercrime, one must first understand the nature of the Internet, online environments, and crime. The emergence and ubiquity of computer technology has led criminological scholarship to engage in some debate over this issue. Specifically, Grabosky (2001) argued that crime in cyberspace is "old wine in new bottles," in that traditional forms of offending are enabled through new tools. For example, criminals can very easily engage in identity theft through *low-tech* methods, such as stealing personal information from mailboxes or during the commission of a robbery or burglary (Allison, Schuck and Lersch 2005). Offenders may also use *high-tech* methods via computers and/ or the internet to obtain personal information that is seemingly unprotected by the victim (Holt and Graves 2007; Newman and Clarke 2003). Computer technology simply provides another medium by which such information can be obtained from potential victims (Grabosky 2001).

Wall (1998), however, argued that the structure and power of virtual environments can be perceived as an issue of "new wine, but no bottles" (Wall 1998, 202). Specifically, the global reach of the Internet enables a scale of connectivity unparalleled in history. People can now form virtual communities that span the globe with speed and efficiency that were previously not possible. Individuals with sexual interests that are considered outside of societal norms quickly adapted to online environments, where they may operate in relative anonymity without fear of shame or social stigma (Rosenmann and Safir 2006). Technology also acts as a force multiplier, in that computing power and automation allow an individual, or "single agent," to engage in crimes that would have previously involved multiple partners (Pease 2001, 24; Wall 2007). This has forced a shift in the social organization of thieving, by decreasing the need for conspirators and divisions of labor, and is leading to a "new 'improved' underworld" where criminals can obtain all manner of resources and engage in crimes (Mann and Sutton 1998, 225; Holt and Lampke 2010). Thus, our traditional models of policing and law must be restructured to adequately deal with the challenges posed by this new environment.

To that end, there is some debate over the terms used to describe crimes involving computers in some fashion. The terms "cybercrime" and "computer crime" have become nearly synonymous, although there is a difference between these two events. Cybercrime refers to crimes "in which the perpetrator uses special knowledge of cyberspace," while computer crimes occur because "the perpetrator uses special knowledge about computer technology" (Furnell 2002, 21; Wall 2001). Despite the differences in these two events, the terms cybercrime and computer crime are frequently treated as interchangeable in popular media and academic literature (Furnell 2002). This work will use the term cybercrime due to the large number of offenses that can occur in online environments and the overwhelming number of computers that are connected to the Internet.

It is important to note, however, that these schemes are rather vague and are not the only definitions used by the law enforcement community. The Federal Bureau of Investigation, for example, does not use the classification cybercrime, only *computer crime*, "where the computer is the victim" (Stephenson 2000, 167). The U.S. Department of Justice uses a similarly open definition: "any violation of criminal law that involved the knowledge of computer technology for its perpetration, investigation, or prosecution" (Conly 1989, 6). These terms are both rather broad and obscure. The U.K. police, however, use a more specific typology that distinguishes between "computer-assisted crimes" and "computer-focused crimes" (Furnell 2002, 22). "Computer-assisted crimes" involve computers in a supporting role in the commission of a crime, although the activity could be performed without computer assistance, while incidents called "computer-focused crimes" are a direct result of computer technology, such as hacking and viruses (Furnell 2002, 22). This typology presents a clearer

explication than other current definitions and illustrates the wide variety of terms used to classify computer crimes.

One of the most comprehensive definitions applied to computer-based crimes was used by the National Institute of Justice (Stambaugh et al. 2001) in their seminal study on the capacity of state and local law enforcement to handle cybercrime. Before conducting this study, the researchers recognized the complex issues surrounding the measurement and definition of computer-based offenses. Thus, they worked in collaboration with state and local agencies to develop a definition of "electronic crime" that refers to:

> fraud, theft, forgery, child pornography or exploitation, stalking, traditional white-collar crimes, privacy violations, illegal drug transactions, espionage, computer intrusions, or any other offenses that occur in an electronic environment for the purpose of economic gain or with the intent to destroy or otherwise inflict harm on another person or institution (Stambaugh et al. 2001, 2).

A similarly broad definition of cyberterrorism was developed, recognizing any "premeditated, politically motivated attack against information systems, computer programs and data ... to disrupt the political, social, or physical infrastructure of the target" (Stambaugh et al. 2001, 2). The wide range of offenses included in these definitions was meant to provide some standard to assess computer-based crime, though it is unclear how much the definition permeates agency and academic definitions of cybercrime.

Some researchers utilize a different method to define cybercrimes through comparisons of the laws made by various countries to identify criminal activity in cyberspace. As legislation against cybercrimes has increased dramatically over the past ten years, some agreement has developed regarding what acts are considered illegal online. For instance, the Global Cyber Law Survey of 50 countries, including nations in Africa, the Americas, Asia, Europe, the Middle East, and Oceania, found 70 percent of countries with laws against computer crimes identified seven specific acts as prohibited (Putnam and Elliott 2001, 37). These acts, considered consensus crimes (based on the agreement in many countries that these activities are criminal), include: unauthorized access, computer-mediated espionage, privacy violations with personal data acquisition or use, damage or theft of computer hardware or software, illicit tampering with files or data, computer or network sabotage including denial-of-service attacks and worms, and the use of information systems to commit fraud, forgery, and "traditional crimes" (Putnam and Elliott 2001, 38).

While comparative law analyses provide a helpful starting point for research, it is important to note that few nations actually define what cybercrimes are, only what behaviors constitute them. Most industrialized countries that are heavily dependent on computers and information networks are the most likely to have laws against computer crimes. Emerging industrial nations are less likely to have developed such legislation, creating safe havens where cyber criminals can operate with minimal risk of extradition (Brenner 2008; Putnam and Elliott 2001). This disparity in codified law adds to the difficulty of defining cybercrimes in a transnational context.

The lack of a clear or universal definition for cybercrime is also related to the significant undercounting of cybercrimes (see Holt 2003; Taylor et al. 2010). Part of this is due to user difficulty in recognizing when cybercrimes occur. Failing computer systems and hardware can mimic criminal acts or the results of criminal activities, obfuscating the situation (Symantec 2003; Stephenson 2000). In fact, almost 25 percent of personal computers around the world that use a variety of security solutions have malicious software, such as a virus, loaded into their memory (PandaLabs 2007). Thus, many individuals are victimized despite the presence and use of antivirus software and other protective programs to defend their system against the random nature of damaging computer attacks.

There are also a range of attacks that can occur in the workplace that may go unreported to law enforcement. Many in the general public believe intrusion attempts come largely from hackers outside of computer networks (Furnell 2002). For example, one estimate of losses due to one form of external attacks called a Denial of Service attack, which keeps others from accessing web based services, was an average of $1.495 million for US companies in 2015 (Ponemon Institute 2015). This massive estimate only reflects attacks that occur since businesses and financial institutions may lose face by reporting compromised systems (see also Holt 2003; Furnell 2002; Nasheri 2005). As a consequence, the true number and losses attributed to external penetration is unknown, but considered to be relatively significant and substantial (Newman and Clarke 2003).

Research involving case studies of insider attacks suggest that hackers may operate within secure environments as trusted system administrators or security professionals (Cappelli, et al. 2006; Dhillon and Moores 2001; Shaw et al. 1998). The actions employees take to misuse or misappropriate resources may go unnoticed, particularly by individuals with administrative privileges (Cappelli et al. 2006; Dhillon and Moores 2001). Insiders may also surreptitiously steal information or place backdoors in programs that can be accessed to cause damage in case they are fired or mistreated (see Cappelli et al. 2006; Shaw et al. 1998). The attacks individuals engage in can be relatively simple in nature and exploit known flaws in internal systems, though some sophisticated intrusions have been documented (see Cappelli et al. 2006). In these situations,

office politics and management may enable cover-ups to occur that can increase the likelihood of non-reporting (see Shaw et al. 1998).

Confusion over where to file reports or complaints also leads to undercounting. As cybercrimes can cross state, territorial, and continental boundaries, jurisdictional issues can arise. In the U.S., for example, the involvement of local or federal law enforcement is dependent upon the crime and the extent of monetary damage to the victim. Unfortunately, many local police departments do not have the tools needed to enforce laws against cybercrime, including knowledge, forensic equipment, and personnel, decreasing the potential for resolution of these crimes (Holt, Burruss, and Bossler, 2015; Stambaugh et al. 2001). Also, if an incident report must be passed from one agency to another after being filed, the likelihood of resolution is further reduced. When expanded to the international level where both the perpetrator and victim are in different nations these problems are even greater in magnitude. Questions develop as to who is responsible for the investigation along with other issues that can negatively affect a case, such as "the number of nations involved, the presence or absence of extreme urgency, the existence of consent and the extent to which the data sought is protected by firewalls, passwords, or encryption" (Putnam and Elliott 2001, 62). These complications make undercounting a considerable problem, particularly at the international level, when coupled with the absence of computer crime laws in some countries.

An even greater obstacle facing researchers is identifying actual statistical measures for cybercrimes. Relatively few countries produce quality data on these offenses, regardless of their level of industrialization. For example, the United States does not provide much data on cybercrimes from a centralized outlet (Holt 2003; Goodman 2001). Such information is notably absent from the FBI's Uniform Crime Report, is not consistently reported in the National Crime Victimization Survey, and is evident in small numbers within the National Incident Based Reporting System (see Holt et al., 2015). As a consequence, there is a significant dark figure of cybercrime that requires further examination in the U.S. and abroad.

Cybercrime Framework

Though there is a paucity of statistics on cybercrime, a growing body of criminological and sociological research has improved our understanding of the forms of cybercrime that exist. One of the most well-referenced and constructed frameworks to understand cybercrimes is Wall's (2001) four-category typology of computer crime to identify the wide range of behaviors encompassed by computer based crimes.

Cyber-Trespass

The first category is cyber-trespass, encompassing the crossing of invisible, yet salient boundaries of ownership online. The most notable cybercriminals engaging in acts of trespass are computer hackers, due to their desire to penetrate computer systems that they do not own (Furnell 2002; Jordan and Taylor 1998). One of the more comprehensive research definitions identifies hackers as those individuals with a profound interest in computers and technology that have used their knowledge to access computer systems for malicious or ethical purposes alike (see Holt 2007; Schell, Dodge and Moutsatsos 2002). The need for the inclusion of ethical applications lies in the fact that the term "hacker" was originally used as a term of respect for programmers in the 1950s and '60s who had significant computer skill (Jordan and Taylor 1998; Levy 1984; Holt 2007). Many in the general public, however, associate modern hackers with costly criminal breaches of computer networks and system boundaries (Furnell 2002; Schell et al. 2002).

Hackers are also responsible for malicious software programs, or malware, that automate a variety of attacks and break into computer systems (Furnell 2002). Malware typically includes computer viruses, worms, and Trojan horse programs that alter functions within computer programs and files. These programs can disrupt email and network operations, access private files, delete or corrupt files, and generally damage computer software and hardware (Taylor et al. 2010). In addition, some forms of malicious software can enable identity theft, fraud, and the loss of personal information (Britz 2004; Taylor et al. 2010). Thus, malware infection poses a significant threat to Internet users around the globe.

The dissemination of viruses across computer networks can be costly due in part to the time spent removing the programs as well as losses in personal productivity and system functions (Symantec Corporation 2003; Taylor et al. 2010). This is reflected in the dollar losses associated with malware, as the average cost to remove malicious code in a US business was $91,500 in 2014 alone (Ponemon Institute 2014). Because of the interconnected nature of computer systems today, an infected system in one country can spread malicious software across the globe and cause even greater damage. The Melissa virus, for example, caused an estimated $80 million in damages around the globe (Taylor et al. 2010). Even responding to false alarms of malware threats is extremely expensive, with the average cost to US businesses at $1.3 million a year

(Ponemon, 2015). Thus, cyber-trespass offenses are a significant concern fo home users, businesses, and governments alike.

Cyber-Deception/Theft

The second and related category within Wall's (2001) typology is cyber- deception and theft. This form of cybercrime includes all the various crimina acquisitions that may occur online, particularly for thefts due to trespass. Th increased use of online banking and shopping sites also allows consumers t transmit sensitive personal and financial information over the Internet (Jame 2005; Newman and Clarke 2003). This information can, however, be surrep titiously obtained by criminals through different methods such as phishin (James 2005; Wall 2007). In a phishing attack, consumers are tricked int transmitting financial information into fraudulent websites, where the infor mation is housed for later fraud (see James 2005; Wall 2007).

In addition, there is an emerging marketplace online where computer crim inals sell and buy information (Franklin et al. 2007; Honeynet Research Al liance 2003; Thomas and Martin 2006). Specifically, Internet Relay Chat, or IRC channels and web forums operate where hackers sell significant volumes o data obtained through phishing, database compromises, and other means. In dividuals in these sites sell credit card and bank accounts, pin numbers, an supporting customer information obtained from victims around the world i lots of tens or hundreds of accounts (Franklin et al. 2007; Holt and Lampk 2010; Honeynet Research Alliance 2003; Thomas and Martin 2006). Some als sell their services as hackers and offer cash out services to obtain physical mone from electronic accounts (Holt and Lampke 2010). As a consequence, crimi nals who frequent these markets can quickly and efficiently engage in credi card fraud and identity theft without any technical knowledge or skill (Frankli et al. 2007; Holt and Lampke 2010; Honeynet Research Alliance 2003; Thoma and Martin 2006). In addition, these markets can lead individuals to be vic timized multiple times without their knowledge.

Beyond theft due to computer intrusions, there are several different type of fraud that are perpetrated online, including electronic auction or retail based fraud schemes, stock scams, and work-at-home plans (Grabosky an Smith 2001; Newman and Clarke 2003). One of the most prevalent and mos costly forms of Internet fraud are advance fee email schemes (Internet Crim Complaint Center 2009; Holt and Graves 2007; Wall 2004). These message are often referred to as "Nigerian" or "419" scams because the emails ofte come from individuals who claim to reside in a foreign country such as Nige ria or other African nations (Buchanan and Grant 2001; Holt and Graves 2007

The sender claims to need assistance transferring a large sum of money out of their country. In return, the sender will share a portion of the sum with the individual who aids them (Holt and Graves 2007). Victims of this type of fraud often lose thousands of dollars on average and may be too embarrassed to report their experiences to law enforcement because of the often obviously false nature of the message they responded to (Buchanan and Grant 2001; Newman and Clarke 2003; Wall 2004).

Another high-profile form of cyber-theft is digital piracy, or the illegal copying of digital media, such as computer software, digital sound recordings, and digital video recordings, without the explicit permission of the copyright holder (Gopal et al. 2004). Such files can be easily downloaded from one of many internet file sharing services or web sites and commonly do not stem from a single user. IDATE (2003) has suggested that illegal file sharing accounts for over four times the amount of official sales of sound recordings worldwide. The same report suggested that peer-to-peer (P2P) file sharing accounts for between 50 and 90 percent of all broadband internet traffic in any given day, depending on the time of day.

The financial losses estimated to result from digital piracy are staggering and participation levels in this illegal activity are commonplace, particularly among college students (Hinduja 2001; 2003; Ingram and Hinduja 2008; Morris and Higgins 2009; Rob and Waldfogel 2006; Zentner 2006). For example, the Motion Picture Association of America (MPAA) reported fiscal losses upwards of $6 billion in 2005 from movie piracy in the U.S. alone. Over 40 percent of these reported losses were argued to be a result of university students in the U.S. (MPAA 2007). In addition, Siwek (2007) reported that the U.S. sound recording industry loses over twelve billion dollars annually due to piracy and another $422 million each year in tax revenue that would have been generated via corporate and personal income taxes (Siwek 2007). Taken as a whole, cyber-deception and theft encompass a wide range of activities, each with significant economic impact.

Cyber-Porn and Obscenity

The third category within Wall's (2001) typology includes cyber-porn and obscenity. Sexually expressive or explicit materials are readily available across the World Wide Web, though they may not be illegal in certain areas (DiMarco 2003; Wall 2001). As a consequence, online pornography has become an extremely lucrative and thriving business (Edelman 2009; Lane 2000). In fact, the adoption and popularity of various forms of media, particularly VHS and DVD media, webcams, digital photography, and streaming web content is in-

timately tied to the pornography industry (Lane 2000). The Internet has dramatically affected the way that pornographic content is distributed, customers are targeted, and amateur stars are made. For example, estimates suggest that the online pornography industry earns over $3,000 per second (Gobry and Saint 2011).

The development of the Internet and computer mediated communications has also fostered the growth of a wide range of communities supportive of deviant sexual behaviors. Those whose sexual preferences are socially marginalized can identify a wide range of resources, such as newsgroups, web forums and list serves where individuals can exchange all sorts of information almost instantaneously (DiMarco 2003). Online spaces also allow individuals to find others who share their interests, creating supportive communities where individuals feel "they are part of a group, from which validation can be drawn, and sexual scripts exchanged" (Rosenmann and Safir 2006, 77). As a consequence subcultures have developed in cyberspace around myriad acts of sexual deviance (DiMarco 2003; Quinn and Forsyth 2005). For example, researchers have explored the practices of individuals interested in bestiality, or sex with animals (Durkin, Forsyth, and Quinn 2006; Maratea 2011), and money slavery, where individuals give money to other individuals in the hopes of receiving sadistic treatment via email or some other electronic medium (Durkin 2007).

The illegal sex trade has also moved to online spaces, such as websites and forums specifically designed for johns to discuss prostitution in cities around the globe (see Holt and Blevins 2007; Hughes 2003; Sharpe and Earle 2003; Soothill and Sanders 2005). Recent research suggests that the clients of prostitutes use the Internet to share information about their real-world experiences with all types of sex workers (Holt and Blevins 2007; Hughes 2003; Sharpe and Earle 2003). Johns reveal their motivations for paying for sex, as well as detailed accounts of their interactions with prostitutes, escorts, and other sex workers. In addition, johns use these methods to describe and warn others about the presence of law enforcement or particularly active community groups in a given area (see Holt, Blevins, and Kuhns 2008). As a result, these online forums can provide insight into the nature of displacement and the methods johns use to obviate the wide range of targeted law enforcement strategies to reduce levels of street prostitution (see Scott and Dedel 2006).

One of the most publicly recognized and feared forms of cybercrime within this framework of cyber-porn and obscenity is pedophilia, where individuals seek out sexual or emotional relationships with children (Jenkins 2001). Recent media attention has focused on the behavior of pedophiles, creating a sort of panic around the number of sexual predators online (Berson 2003; McKenna and Bargh 2000). In fact, the number of arrests for child pornography possession has increase substantially over the last decade, with over 3,700 arrests in 2009 alone (Wolack, Finkelhor, and Mitchell 2012). Criminological research has provided significant insight into the ways pedophiles use the Internet as a means to facilitate criminal behavior (Durkin 1996, 1997; Durkin and Bryant 1999; Jenkins 2001; Quayle and Taylor 2002). For example, the Internet is a vehicle for the identification, trade, and distribution of pornographic and sexual materials, including comic books, stories, pictures, and films (Durkin 1997; Jenkins 2001; Fontana-Rosa 2001; Quayle and Taylor 2002). In addition, computer-mediated communications provide a wealth of potential victims that can be groomed for sexual contact offline (see Wolack, Finkelhor and Mitchell 2003; Wolack, Mitchell and Finkelhor 2004).

The Internet also provides a mechanism for pedophiles to identify and talk with others through usergroups, web forums, and chatrooms (Durkin 1996, 1997; Durkin and Bryant 1999; Holt, Blevins, and Burkert 2010). These sites provide a way for pedophiles to come together to validate their sexual interests, share information about their habits, and find support for their behaviors (Durkin and Bryant 1999; Jenkins 2001). Exchanges between individuals provide information on the ways individuals become interested in relationships with children and how to justify these behaviors (Durkin and Bryant 1999; Holt et al. 2010). For example, online communities often use the term "child love" to refer to their attractions, rather than the more derogatory and stigmatizing word "pedophile" (Durkin 1997; Holt et al. 2010; Jenkins 2001).

Cyber-Violence

The final form of crime within Wall's (2001) typology is cyber-violence, representing the distribution of a variety of injurious, hurtful, or dangerous materials online. For example, individuals have begun to use the Internet as a means to harass or bully others (Bocij 2004; Finn 2004; Holt and Bossler 2009). Harassment can take various forms, such as threatening or sexual messages delivered to an individual privately via email, instant messaging services, or cell phone (see Bocij 2004). The emergence and popularity of social networking websites like Facebook, however, allow individuals to post threatening or hurtful content in public settings for anyone and everyone to see (see Hinduja and Patchin 2009). The victims of such harassing communications respond in a variety of ways; some view these messages to be nothing more than a nuisance, while others experience significant physical or emotional stress, including depressive symptoms and suicidal ideation (Finkelhor et al. 2000; Finn 2004; Hinduja and Patchin 2009). Estimates of online harassment and stalking appear to be on the rise, particularly among adolescent

and young adult populations, due in part to frequent Internet use (Boci
2004; Finn 2004; Hinduja and Patchin 2009; Holt and Bossler 2009; Jones
Mitchell, and Finkelhor 2012). For example, a recent national examination
of young Internet users found that 11 percent of the sample experienced
some form of harassment while online, which is a 50 percent increase over
the last decade (Jones et al. 2012). In addition, evidence suggests that hav-
ing peers who engage in cybercrime increases an individual's risk of harass-
ment (Hinduja and Patchin 2009; Holt and Bossler 2009). Thus, the risk o
online violence may share similar correlates with real-world violence (Hol
and Bossler 2009).

The Internet has also become an important resource for political and so-
cial movements of all types. Mainstream and alternative political and socia
movements have grown to depend on the Internet to broadcast their ideolo
gies across the world. Groups have employed a range of tactics depending on
the severity of the perceived injustice or wrong that have been performed (see
Jordan and Taylor 2004). Often, these virtual efforts develop in tandem with
real-world protests and demonstrations (see Jordan and Taylor 2004). A con-
flict developed between Russian and Estonian factions in April 2007 when the
Estonian government removed a Russian war monument from a memorial
garden in a national cemetery (Brenner, 2008; Jaffe 2006; Landler and Markoff
2007). Russian citizens living in Estonia protests in the streets leading to over
1,000 arrests of Russians living in the country. The conflict quickly grew into
online spaces, with hackers in both Estonia and Russia attempting to engage
in different hacks and spam campaigns (Brenner, 2008; Jaffe, 2006). As a con-
sequence, Russian attacks were able to shut down critical components of Es-
tonia's financial and government networks, causing significant economic harm
to citizens and industry alike (Brenner, 2008; Landler and Markoff, 2007).
Multiple Estonian banks lost millions of dollars due to DDoS attacks which
make their services unavailable for hours (Landler and Markoff, 2007).

Politically-driven groups have also employed hacking techniques to engage
in more serious strikes against governments and political organizations (see
Furnell 2002). These actions are sometimes called "hacktivism," as the "hack"
or attack is used to promote an activist agenda or express an opinion (Furnell
2002, 44). Their actions may, however, violate the law and produce fear or
concern among the general population (Jordan and Taylor 2004). For instance,
the activist group Anonymous and its more radical offshoot LulzSec began tar-
geting government and industry targets online in order to express their dis-
sent against attempts to limit the availability of pirated media and against
general corruption (Correll 2011). Their attacks ranged from Denial of Serv-
ice attacks to mass compromises of sensitive information from law enforce-

ment and industrial service providers. At the same time, various groups in
support of Al-Qaeda operate web forums to distribute hacker tools and coor-
dinate attacks. One such hacker named Younis Tsouli promoted the use of
hacking tools against various targets in support of global jihad under the han-
dle Irhabi 007, or Terrorist 007 (Denning 2011). He posted a manual titled
"The Encyclopedia of Hacking the Zionist and Crusader Websites," which de-
tailed various attack methodologies and a list of vulnerable targets online in order
to disrupt online systems of Western nations (Denning 2011). Thus, there are
significant risks and threats from politically motivated crimes online.

The Structure of This Book and Its Contributions

Taken as a whole, there is a need for a diverse body of research to under-
stand the correlates and causes of cybercrime, as well as shifts in deviant be-
havior that can occur over time as a consequence of technology and the Internet
(see also Holt 2007; Mann and Sutton 1998; Quinn and Forsythe 2005). The
various chapters of this book discuss these issues in depth by exploring the
spectrum of cybercrimes in detail. The organization of this book follows the
structure of Wall's (2001) typology by focusing on cyber-trespass, deception,
obscenity, and violence.

In Chapter Two, Patrick Kinkade and his colleagues explore the subculture
of hacking through an ethnography of attendees at a hacker conference. Com-
puter hacking is unique in that most all offenses take place virtually, though
individuals may have relationships with deviant peers in the real world and
online. Few have explored the dynamics of hacker relationships in the real
world, thus this chapter provides a much needed investigation of the way in
which hackers engage one another and the way that this shapes the experience
of hacking generally.

Johnny Nhan provides an overview of the legal responses to the related
problem of digital piracy in Chapter Three. Specifically, this section discusses
the evolution of the problem of music piracy as a form of cyber-theft over
time. Not only have the tactics of pirates changed along with technological
shifts, but so have the legislative and law enforcement practices to combat
piracy. Thus, this paper provides a careful historical review of the difficulties
inherent in combating cybercrime and the complexities of balancing freedom
of information with controls.

In Chapter Four, Sarah Turner and her colleagues considér the problem of
spam-driven work-at-home fraud schemes. The authors examine this rela-

tively common form of fraud and the way in which spam messages are structured to entice individuals to respond, from the written content of the initial email to any external websites that the sender may link to online. Their investigation demonstrates that spam distributors can easily structure messages to convince prospective recipients to respond in such a way as to increase their risk of fraud victimization.

Alice Hutchings considers hacking and fraud through an assessment of criminological theory in Chapter Five. This section attempts to integrate various theories through a qualitative study of law enforcement and offenders' opinions on these issues. The findings highlight the factors that may lead individuals to engage in cybercrime over time.

Though hackers and data thieves generate significant public concern, they receive much less attention than the activities of pedophiles and child pornographers in online environments. There is significant fear over the presence of child predators in cyberspace, which has spurred a variety of social science research to understand this problem. Marcus Rogers and Kathryn Seigfried-Spellar elaborate on this issue in Chapter Six through a discussion of frameworks to understand pedophilia and child pornography users and creators. They argue that the existing typologies used to investigate and prosecute child pornography in various countries do not adequately account for the role of technology in the acquisition and use of these materials. Rogers and Seigfried-Spellar provide their own framework in this chapter and detail how it can be used to better combat this problem.

In Chapter Seven, Christine Milrod provides a detailed discussion of her experiences as a sex therapist in a prostitute review website. As a professional her experiences demonstrate the practices of both the customers and workers involved in the sex trade, and the ways that the Internet are affecting prostitution on and offline.

The use of technology to facilitate sexual activities and interests are also related to the most common forms of cyber-violence. Billy Henson and Bradford Reyns detail the problem of cyberstalking in Chapter Eight, with a distinct focus on the available research literature of both victims and offenders. They provide a robust discussion of how this problem is defined and the prevalence of cyberstalking victimization among multiple populations.

Marjie Britz provides a critical overview on the most problematic and nebulous form of cyberviolence in Chapter Nine: cyberterror. She notes that there is no single definition for this term, though various activities have been labeled as cyberterror. Britz provides an overview of the research literature on this issue from the social and military sciences and gives various examples of terror incidents to give context to this phenomenon.

In Chapter Ten, Aunshul Rege provides a detailed exposition of a pertinent target for both hackers and cyber-terrorists: industrial control systems. These systems are used to manage and remotely control water, power, and electrical systems, but could be easily compromised and impacted by malicious actors acting on behalf of an extremist group or nation-state. Rege gives a carefully considered examination of these systems and the ways that attackers have or may harm systems in the future.

References

Abelson, Reed, and Julie Creswell. Data breach at Anthem may forecast a trend. *The New York Times*, Feb. 6, 2015. Accessed March 30, 2015. http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html?_r=0.

Allison, Stuart F.H., Amie M. Schuck, and Kim Michelle Lersch. "Exploring the crime of identity theft: prevalence, clearance rates, and victim/ offender characteristics," *Journal of Criminal Justice* 33 (2005): 19–29.

AVN Media Network. "Industry Stats," Accessed February 1, 2009. http://www.avnmedianetwork.com/index.php?content_about_industrybuzz.

Berson, Ilene R. "Grooming cybervictims: The psychosocial effects of online exploitation of youth," *Journal of School Violence* 2 (2003): 5–18.

Bocij, Paul. *Cyberstalking: Harassment in the Internet age and how to protect your family.* Westport: Praeger, 2004.

Bossler, Adam M. and Thomas J. Holt. "On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory," *The International Journal of Cyber Criminology* 3 (2009): 400–420.

Brenner, Bill. Banks prepare lawsuit over TJX data breach, 2007. Accessed October 7, 2008. http://searchfinancialsecurity.techtarget.com/news/article/0,289142,sid185_gci1294453,00.html.

Brenner, Susan W. *Cyberthreats: The Emerging Fault Lines of the Nation State.* New York: Oxford University Press, 2008.

Britz, Marjie T. *Computer Forensics and Cybercrime: An Introduction.* Upper Saddle River, NJ: Prentice Hall, 2004.

Buchanan, Jim, and Alex J. Grant. "Investigating and Prosecuting Nigerian Fraud," *United States Attorneys' Bulletin*, November (2001), 29–47.

Cappelli, Dawn, Andrew Moore, Timothy J. Shimeall, and Randall Trzeciak. 2006. *Common Sense Guide to Prevention and Detection of Insider Threats.* Pittsburg, PA: Carnegie Mellon Cylab, 2006. Accessed November 1, 2007. http://www.us-cert.gov/reading_room/prevent_detect_insiderthreat0504.pdf.