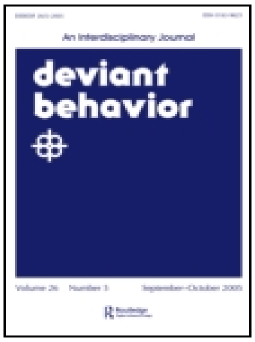

Deviant Behavior

ISSN: 0163-9625 (Print) 1521-0456 (Online) Journal homepage: https://www.tandfonline.com/loi/udbh20

An Assessment of the Current State of Cybercrime Scholarship

Thomas J. Holt & Adam M. Bossler

Deviant Behavior, 35: 20–40, 2014
Copyright © Taylor & Francis Group, LLC
ISSN: 0163-9625 print / 1521-0456 online
DOI: 10.1080/01639625.2013.822209

An Assessment of the Current State of Cybercrime Scholarship

Thomas J. Holt

School of Criminal Justice, Michigan State University, East Lansing, Michigan, USA

Adam M. Bossler

Department of Criminal Justice and Criminology, Georgia Southern University, Statesboro, Georgia, USA

Computers and the Internet have become a vital part of modern life across the world, affecting communications, finance, and governance. At the same time, technology has created unparalleled opportunities for crime and deviance on- and off-line. Criminological research has expanded its focus over the last two decades to address the various forms of technology-enabled crime and the applicability of traditional theories to account for offending. There is, however, a need for careful consideration of the state of the field in order to identify issues requiring further study and analysis. This study examines the current literature on virtually all forms of cybercrime and the theoretical frameworks used to address these issues. In turn, we hope to give direction to refine our understanding of criminological theory and social policies to combat these offenses.

Over the last two decades, a massive shift in the ways that humans utilize computer technology has occurred. The development of the World Wide Web and easy-to-use computer hardware and software revolutionized the way in which people communicate and engage in business transactions (Newman and Clarke 2003; Wall 2007). The development of cellular telephony, wireless Internet connectivity, tablet PCs, and mobile devices made it increasingly easy for individuals to go on-line from anywhere at any time.

These innovations spurred massive changes in our perceptions of personal expression and social interaction. For instance, Facebook, Twitter, and other social networking sites have become the preferred communications vehicle for individuals between the ages of 18 and 34 (Socialbakers 2011). Consumers are also increasingly using technology in order to shop and identify products at discounted rates, such that 60% of the United States population now purchases an item on-line at least once per fiscal quarter (Anderson 2010). Computers and the Internet now serve as the backbone for virtually all facets of modern life, from personal communications and finance to the processing and management of electrical grids and power plants (Brenner 2008; Brodsky and Radvanovsky 2011; Rege 2013).

Received 3 January 2013; accepted 30 April 2013.

Address correspondence to Thomas J. Holt, School of Criminal Justice, Michigan State University, 434 Baker Hall, East Lansing, MI 48824, USA. E-mail: holtt@msu.edu

As a consequence, there are now myriad opportunities for individuals to misuse these devices to engage in acts of deviance and crime. Indeed, the amount of cybercrime has grown tremendously. While there is no single, agreed-on definition of cybercrime, many scholars argue that it involves the use of cyberspace or computer technology to facilitate acts of crime and deviance (Grabosky 2001; Wall 2007). The World Wide Web and cellular telephony are being used by the customers of prostitutes to discuss the sex trade and facilitate encounters with sex workers (Holt and Blevins 2007; Milrod and Wietzer 2012; Sharp and Earle 2003). Fraudsters use bulk e-mail to send out a variety of get-rich quick schemes to entice victims (Grabosky et al. 2001; James 2005; King and Thomas 2009). These electronic resources are being incorporated by youth to engage in bullying and social harm against their classmates (Hinduja and Patchin 2009; Wolak et al. 2012). Technology has also enabled new offenses that were not otherwise possible, such as the distribution of malicious software and hacking that can cause substantive economic harm and the loss of sensitive personal data and intellectual property (Bossler and Holt 2009; Choi 2008; Holt and Turner 2012).

Criminological research has expanded its focus over the last two decades to improve our understanding of the impact of technology on the practices of offenders, factors affecting the risk of victimization, and the applicability of traditional theories of crime to virtual offenses (Taylor et al. 2010). The body of scholarship that has emerged has greatly improved our knowledge of technology-enabled crime, though there is a need for a systematic review of the literature due to the range of methodological and theoretical perspectives that have been employed. Qualitative researchers have begun to develop innovative on-line data sets to examine offending populations in virtual spaces (see Holt 2010 for review). Quantitative methods employed by researchers have ranged from binary logistic and multiple regression models generated from convenience samples of college students (e.g., Higgins 2005; Holt and Bossler 2009), to structural equation modeling techniques (Higgins et al. 2006), to a small number of descriptive analyses of large nationally representative samples of youth (Jones et al. 2012). Researchers have also applied various traditional criminological theories to multiple forms of cybercrime with distinct operationalizations making it difficult to assess their overall impact on the field.

Here we assess the existing literature on various forms of technology-enabled crime using Wall's (2001) four category cybercrime typology: (1) cyber-trespass; (2) cyber-deception/theft; (3) cyber-porn and obscenity; and (4) cyberviolence. This is considered one of the most comprehensive frameworks to understand the incorporation of technology into various forms of offending. We will explore each category in detail and provide recommendations for future research within each category to demonstrate areas of expansion and clarification. In turn, we hope this will refine our knowledge of cybercrime, criminological theory, and positions for social policy.

Cyber-Trespass

The first category within Wall's (2001) typology is cyber-trespass, which encompasses the crossing of invisible, yet salient boundaries of ownership on-line. Specifically, if an individual attempts to access a computer system, network, or data source, without the permission of the system owner, they are violating a recognized border of ownership. These activities are most closely associated with computer hackers who often attempt to access the networks and computer systems owned by individuals, citizens, and governments. In fact, computer hackers are primarily recognized for their role in malicious attacks against computer systems and sensitive networks (Holt 2007; Jordan and Taylor 1998; Schell and Dodge 2002). Hackers are also responsible for malicious software programs, such as viruses and botnet code, which automate a variety of attacks and break into computer systems (Chu et al. 2010). Malicious programs can disrupt network traffic, capture passwords for sensitive resources, delete or corrupt files, and utilize infected systems for future attacks (Symantec Corporation 2012).

While there have been no nationally representative studies assessing involvement in hacking among juvenile populations, research from college samples suggest that between 10 and 15% of individuals engage in password guessing (Bossler and Burruss 2011; Holt et al. 2010a; Rogers et al. 2006; Skinner and Fream 1997), although less than 5% engage in more serious forms of this activity like malware creation (Rogers et al. 2006). These figures are useful to understand the prevalence of hacking, although they do little to improve our knowledge of the reasons why so few engage in these activities. Thus, several qualitative researchers have expanded our understanding of the complexities of hacking and the dynamics of hacking attacks by either interviewing individuals who self-identify as hackers or collecting information from forum data sources (e.g., Holt 2007; Jordan and Taylor 1998; Taylor 1999). Unfortunately, these qualitative studies do not have the ability to estimate the number of individuals who commit hacker-like behaviors. Thus, a blend of quantitative and qualitative studies is necessary to understand both the prevalence and causes of hacking behavior.

The exploration of the computer hacker subculture using qualitative data sources has been the primary avenue of research within this subcategory. These studies suggest hackers operate in a subculture that emphasizes both a profound connection to and deep knowledge of technology as well as demonstrations of mastery of computer technology and the social scene (Holt 2007; Jordan and Taylor 1998; Taylor 1999). In addition, research has identified several predictors for participation in hacking. First and foremost, many hackers report exposure to technology early on in life, whether through playing video games or simple communications (Holt 2007; Schell and Dodge 2002; Taylor 1999). Many hackers also describe having a curiosity of technology that drives them to understand how technologies work at fundamental levels (Holt 2007; Jordan and Taylor 1998; Taylor 1999). Evidence also suggests that hackers have some capacity for self-management, though some report Type A personalities and anti-social tendencies. They also have higher creative scores on personality assessments and some analytic decision-making processes (Rogers et al. 2006; Schell and Dodge 2002).

Hackers also consistently report maintaining peer relationships with other hackers, whether on- or off-line (Holt 2009; Holt and Kilger 2008; Schell and Dodge 2002). It is unclear whether virtual or real peer relationships have a greater impact on real world behavior, as most studies do not assess variations in the quantity and value individuals place on peers across the digital divide. Limited research using on-line data sources and social network analysis techniques demonstrate skilled hackers are central to larger social networks of less skilled actors (Decary-Hetu and Dupont 2012). Qualitative research suggests that virtual peer groups may be more significant because hackers may be unable to identify others in the real world who share their interests (Holt 2009; Holt and Kilger 2008; Schell and Dodge 2002). Regardless, peer relationships are correlated with involvement in hacking activities generally (Bossler and Burruss 2011; Holt 2009; Holt et al. 2010a; Skinner and Fream 1997).

In fact, peer associations are pivotal to the introduction and acceptance of techniques of neutralization to excuse or justify malicious or unethical behaviors (Bossler and Burruss 2011; Holt et al. 2010a; Skinner and Fream 1997). Gordon (2000) found that virus writers were often not concerned with the effects of their viruses, even if they knew that they were illegal and harmful. Hackers argue that their actions do not necessarily cause harm (Gordon and Qingxiong 2003). They may alternatively blame victims for having poor skill or security to prevent victimization (Jordan and Taylor 1998; Taylor 1999). Similarly, peer relationships reinforce the perception that participation in hacking and piracy are acceptable, which may in turn increase the likelihood of future offending (Bossler and Burruss 2011; Holt et al. 2010a; Skinner and Fream 1997).

In addition to deviant peer relationships, recent research has also begun to consider the role of self-control on the likelihood of involvement in hacking (Bossler and Burruss 2011; Gordon and Qingxiong 2003; Holt et al. 2012; Holt and Kilger 2008). Gottfredson and Hirschi's (1990) General Theory of Crime argues that individuals with low self-control are impulsive, insensitive, non-verbal, present-oriented risk-takers who prefer simple tasks. As a consequence, they are unable to fully consider the consequences and benefits of their actions, making them more likely to engage in crime and risky behavior. Although this theory has substantial support across myriad studies of traditional street crimes (Pratt and Cullen 2000), it is not clear what role self-control may play in computer hacking due to the range of attacks that can be labeled as a hack (Bossler and Burruss 2011; Holt and Kilger 2008). Simple forms of hacking such as guessing someone's password to gain access to an account involves virtually no technical sophistication and can be achieved through persistent guessing. At the same time, more serious and technologically sophisticated offenses such as malware production require a great deal of technical proficiency and time spent researching and developing tools.

As a result, the impact of self-control may vary based on the overall skills and attitude of the hacker. Holt and Kilger (2008) found that hackers in both college settings and in the general population had relatively high levels of self-control. Recent research by Bossler and Burruss (2011) found an interesting relationship between self-control, peers, and hacking. Specifically, hackers who had no peer relationships to other hackers reported higher levels of self-control. Individuals with peers who hacked had lower levels of self-control and benefitted from social relationships to reinforce their activities and learn methods of hacking (Bossler and Burruss 2011). Holt and colleagues (2012) found in a sample of middle and high school students that having deviant peer associations exacerbated the effect of low self-control on cyberdeviance in general, but that the significant interaction effect was not found for any of the five types of cybercrime they examined, including hacking.

These findings provide interesting insights into the applicability of traditional criminological theories to account for hacking. Those hackers with low self-control may initially take an interest in hacking because they recognize the opportunity to engage in a risky behavior through relatively simple acts like password cracking. Over time, however, they may be unable to move beyond basic attacks due to an inability to concentrate and better understand the complex nature of certain hacks. Those with higher levels of self-control may not necessarily face these problems as they can hone their knowledge and skill over time. This theoretical issue requires much greater exposition with more sophisticated measures of hacking in larger populations in order to clarify the relationship between low self-control, peer relationships, and hacking.

Although the body of scholarship on the correlates of participation in hacking is growing, little research has been conducted that applies existing theories to more complex forms of hacking such as malicious software use or creation (Bossler and Burruss 2011; Gordon and Qingxiong 2003). A relatively small proportion of individuals may engage in these behaviors due to the technical knowledge needed to successfully use them in hacking attacks. Thus, additional research is needed with larger purposive sampling techniques from both juvenile and adult samples to understand the prevalence and prospective predictors for involvement in these behaviors.

A similar dearth of research exists that identifies the risk factors associated with cyber-tresspass victimization. This is due in part to the difficulties in identifying victims of computer hacking and certain forms of cybercrime (Bossler and Holt 2009, 2010; Yar 2005). Victims may not know that they have been attacked since malicious software infections can mimic failing computer systems and hardware (Bossler and Holt 2009, 2010; Symantec Corporation 2012). In addition, individuals may only realize that some sort of hack has affected them after information has been removed or corrupted in some fashion (Wall 2007). Finally, when a compromise or attack occurs, it may go unreported to law enforcement due to concerns over whether it will be taken seriously or if anyone can investigate the offense at all (Brenner 2008; Wall 2001).

As a consequence, most criminological research utilizes self-report data from college samples to assess the correlates of malware and hacking victimization (Bossler and Holt 2009, 2010; Choi 2008). These studies commonly use routine activity frameworks to identify correlates for victimization with mixed success (Bossler and Holt 2009; Choi 2008; Ngo and Paternoster 2011). This may stem from the nature of hacking and compromise, in that hackers will generally attempt to compromise large populations of computer users rather than very targeted attacks against specific individuals (Chu et al. 2010; Gordon and Qingxiong 2003). To that end, there is mixed evidence that women are more likely to experience computer hacking victimization or malware infections (Bossler and Holt 2009, 2010; Ngo and Paternoster 2011). There is, however, no significant relationship between age and the risk of victimization, suggesting that target suitability factors may not generally apply to hacking offenses (Bossler and Holt 2009; Ngo and Paternoster 2011). Individual participation in cybercrimes are strongly correlated with the risk of victimization, especially pirating media or viewing on-line pornography (Bossler and Holt 2009; Choi 2008; Holt and Copes 2010; Wolfe et al. 2007). Peer involvement in cybercrime also increases individual risk of victimization through secondary exposure to malware infections generally (Bossler and Holt 2009, 2010).

The evidence supporting the ability of physical and social guardians to reduce the risk of cyber-tresspass victimization can be considered mixed at best (Bossler and Holt 2009; Choi 2008; Ngo and Paternoster 2011). Various computer-based protective software suites have been engineered to reduce the likelihood of infection, such as anti-virus, anti-spyware, and adware programs designed to scan system files (PandaLabs 2007; Symantec Corporation 2012). These software utilize signature-based definitions that can identify malicious files while they are being downloaded or remediate infections and corrupted files after an infection has occurred (Symantec Corporation 2012; Taylor et al. 2010). Their utility in the literature, however, is inconsistent as Choi (2008) found users with computer security software had a reduced risk of malware victimization. Ngo and Paternoster (2011) found that users with protective software were more likely to report infections, while Bossler and Holt (2009) found no relationship between security programs and risk. Similarly, personal computer skills had no relationship to the risk of malware infections (Bossler and Holt 2009; Ngo and Paternoster 2011).

The inconsistent findings present in the victimization literature may stem from the consistent use of cross-sectional research designs (Bossler and Holt 2009; Choi 2008; Ngo and Paternoster 2011). The use of a single data point makes it difficult to determine when an individual gains access to protective software relative to an infection or compromise. Furthermore, individuals who have greater technological skill may be more apt to recognize when an attack has taken place, artificially affecting the relationship between protective factors and victimization. Alternatively, those who have antivirus programs may be more capable of recognizing an attack, thereby artificially conflating the risk of infection in cross-sectional studies.

Taken as a whole, there is a need for research to improve our understanding of the correlates of malware infection victimization. Longitudinal research is needed to better identify the correlates of victimization and the influence that a compromise may have on user behavior over the short and long term. In addition, alternative operationalizations for infection and compromise are needed to expand our ability to measure victimization. Currently, most studies use a single measure based on self-identified data loss or compromise (Bossler and Holt 2009; Choi 2008; Ngo and Paternoster 2011). Since victimization can occur without the users' knowledge, it is critical that researchers use measures that reflect errors or malfunctions in hardware and software that may reflect when a compromise has taken place (see Pew Internet and American Life 2005). This can refine our knowledge of the prevalence and incidence of malware infection victimization, as well as improve our knowledge of the correlates of cyber-trespass crimes generally.

Cyber-Deception/Theft

The second category of Wall's (2001) typology is cyber-deception and theft, which includes the use of the Internet to steal information or illegally acquire items of value, whether from individuals or corporations. This category is innately tied to cyber-trespass since malicious hackers frequently attempt to capture sensitive information and data through trespassing. Hackers are increasingly targeting data repositories managed by financial institutions and on-line retailers to steal large amounts of data through a small number of compromises. For example, the Heartland Payment Systems breach consisted of 130 million credit and debit cards stolen in a matter of months (Verini 2010). Although there are no single source agencies that report on data breaches, the Verison (2012) report on global breaches suggests that 855 data breaches occurred in 2011 with 174 million consumer records lost in the process. This is an increase over previous years and appears driven overwhelmingly by hacking and malware tools (Verison 2012). Unfortunately, there are no immediate estimates for the cost of large scale data breaches for individual consumers as their data may or may not be abused by an attacker (Verini 2010). In much the same way, corporations do not typically provide loss metrics for the cost of breaches due to embarrassment over the losses and variations in the attack methods employed by the actors (Verison 2012).

Cyber-deception/theft also includes two offense types that are made easier by, but do not require, technology in order to perform. First, fraudsters have adopted various fraud schemes to on-line environments, such as the Nigerian or 419 messages and work-at-home schemes (Grabosky et al. 2001; Holt and Graves 2007; King and Thomas 2009; Newman and Clarke 2003). These schemes are facilitated through the use of spam e-mail to access as wide a population as possible and easily manipulate susceptible populations. Statistics on the losses associated with these crimes, or their general prevalence, are not consistent due to the lack of standardized reporting agencies and victim awareness of these offenses. The Internet Crime Complaint Center (2012) found the most common complaint involves scams that appear to originate from the FBI or another government agency. The average victim loses $245 per incident. Victims of work-at-home scams lost an average of $1,160 per complaint (IC3 2012), while respondents of advance fee frauds lost approximately $1,500 per complaint (NWC3 2010).

The second offense type is digital piracy, or the copying of digital media such as computer software, sound and video recordings, and other materials without the explicit permission of the copyright holder (Higgins 2005; Hinduja 2003). Consumers have been able to copy intellectual property prior to the development of the MP3 and other forms of digital compression (see Taylor 1999). The emergence of the Internet and computer technology, however, simplified the process of sharing and accessing pirated media (Bachmann 2007; Nhan 2013). Cost estimates related to digital piracy are not easy to validate. For instance, a study by the Business Software Alliance (2012) found that software piracy cost the industry $63.4 billion dollars worldwide in 2011, with the largest losses in the United States at $9.8 billion despite having legitimate software sales at $41 billion. Similarly, losses for music and movie piracy appear to be in the billions of dollars every year (Siwek 2007; The Numbers Guy 2013).

Research pertaining to various forms of cyber-theft has increased substantially over the last decade. Several qualitative studies have used content analysis techniques to examine the content of Nigerian or 419 scam e-mails (Holt and Graves 2007; King and Thomas 2009), phishing scams (Huang and Brockmann 2010), and work-at-home schemes (Grabosky et al. 2001; Turner et al. 2013). These studies clearly demonstrate that scammers are careful to construct messages that prey on victims' emotions by using language pertaining to religion or framing the respondent in the context of a caring person. The desire to gain a substantial profit through minimal investment is also prominently featured in order to entice responses. While these studies provide valuable insights into the ways that scammers' structure messages, they are largely atheoretical and do little to expand our understanding of the prospective correlates of involvement in on-line fraud.

In addition, little research has been conducted on the victims of on-line fraud schemes due to the limited reporting of these crimes. The Internet Crime Complaint Center (IC3 2012) is one of the few resources available for victims to report their experiences (Holt and Graves 2007). The limited body of scholarship regarding on-line fraud victimization suggests that there are few consistent demographic predictors due to the wide net cast by fraudsters (Holtfretter et al. 2008; Newman and Clarke 2003; Pratt et al. 2010). Based on data from the Internet Crime Complaint Center (IC3 2012), however, it appears that those under the age of 20 are less likely to respond to various e-mail-based scams (IC3 2012). In addition, males and females vary in their responses to certain schemes. Females are more likely to respond to romance scams, while males respond at higher rates to FBI impersonation scams (IC3 2012). It is really unknown, however, how technological sophistication and other behavioral and attitudinal factors affect the risk of victimization.

Scholars have also spent little time examining the applicability of traditional criminological theories in explaining on-line fraud victimization. Low self-control appears to have limited utility to account for credit card fraud victimization (Bossler and Holt 2010), which may again stem from the broad targeting practices of fraudsters. Instead, on-line routine activities appear to increase the risk of fraud targeting, specifically buying items through websites and the time a person spends on-line (Holt and Turner 2012; Pratt et al. 2010). The small scope of research in this area, however, requires a great deal of future research in order to validate the notion that behavior is more significant than demographics in the general risk of on-line victimization.

In contrast to traditional forms of cyberfraud, the research literature surrounding involvement in digital piracy is quite large and continually growing (see Higgins and Marcum 2011). In fact, digital piracy may be the most frequently studied form of cybercrime within the field of criminology at the moment. Though there is substantive complexity in measuring the economic losses of piracy, social scientists have been more effective in assessing the prevalence and causes of piracy, especially in college samples. These studies generally find the most significant predictor for digital piracy to be associations with peers who engage in piracy (Higgins 2005; Higgins and Marcum 2011; Higgins et al. 2012; Hinduja and Ingram 2008; Holt et al. 2012; Skinner and Fream 1997). This may be a function of the basic technological skill needed to engage in simple forms of piracy. Individuals may acquire initial models or sources of imitation for piracy through peer associations (Hinduja 2003; Holt and Copes 2010; Skinner and Fream 1997). The need for these associations declines with time, however, as piracy becomes easier to complete.

In addition, definitions favoring the violation of computer software laws and techniques of neutralization that diminish personal responsibility are correlated with the commission or intent to pirate software (Higgins and Marcum 2011; Ingram and Hinduja 2008; Skinner and Fream 1997; Steinmetz and Tunnell 2013). Most often, individuals rationalize piracy based on the perception that there is minimal economic injury to artists or corporations, as well as no real victim because of the lack of harm stemming from piracy (Higgins and Marcum 2011; Ingram and Hinduja 2008). Similarly, individuals are more likely to pirate materials when they feel minimal responsibility for their downloading behaviors because they perceive there to be no rules concerning digital piracy and have easy and immediate access to pirated materials (Higgins and Marcum 2011; Ingram and Hinduja 2008; Steinmetz and Tunnell 2013). It is important to note that most existing social learning studies examining piracy do not include measures for all four components of the social learning process. Imitation and differential reinforcement are frequently absent in assessments of digital piracy, though they appear to have an influence on behavior. Specifically, positive reinforcement for participation in software piracy (Ingram and Hinduja 2008) and the presence of sources of imitation for pirating behaviors increase the likelihood that an individual will engage in piracy (Holt et al. 2010a; Ingram and Hinduja 2008; Skinner and Fream 1997).

Low self-control also appears to be a substantive predictor for involvement in piracy, whether involving music (Higgins et al. 2012; Hinduja and Ingram 2008), movies (Higgins et al. 2006), or software (Higgins 2005). Additionally, this relationship is present across college (Higgins and Marcum 2011) and juvenile populations (Holt et al. 2012). This is sensible in that piracy enables immediate and relatively easy access to a desired commodity with virtually no cost to the offender. In addition, multiple studies have found those who engage in piracy to have little respect or concern for user agreements and the financial impact of their downloading activities (Higgins 2005; Higgins et al. 2006; Holt and Copes 2010), reflecting basic components of low self-control.

Since most studies of digital piracy incorporate aspects of both social learning theory and the general theory of crime, it is important to note that all of these variables tend to remain significant when included together in a single model. In fact, many studies have found that the effect of low self-control on piracy is neither affected by peer associations nor acceptance of definitions supportive of piracy behaviors (Higgins and Marcum 2011). As a consequence, some theorists have argued that the components of each theory must be included in order to avoid model misspecification (Higgins and Marcum 2011; Pratt and Cullen 2000; Pratt et al. 2009). It is unclear if this is an appropriate form of theoretical integration due to the evidence supporting the mediating effect of social learning between low self-control and cybercrime (Bossler and Holt 2010;

Burruss et al. 2012) and the lack of empirical studies including full operationalizations of the social learning process.

There are still various questions that must be addressed with regard to digital piracy, particularly the deterrent effects of legal sanctions on involvement in piracy. Bachmann (2007) found that a reduction in piracy rates during a two year period was temporary despite a sweeping anti-piracy campaign by the Recording Industry Association of America. His study utilized multiple macro-level data sources, though there have been no attempts to replicate the findings. Other researchers have considered the deterrent effect of extralegal sanctions, such as malware infections, as a consequence of downloading corrupted pirated materials (Holt and Copes, 2010; Wolfe et al. 2007). Such research is vital to improve our understanding of the impact of traditional campaigns to reduce individual involvement in piracy. Furthermore, there have been few studies examining piracy from the perspective of copyright holders and performers. Such insights would prove useful in assessing the economic, social, and psychological harm felt by prospective victims of piracy.

Cyber-Porn and Obscenity

The third category of Wall's (2001) cybercrime typology is cyber-porn and obscenity. This category encompasses the range of sexual expression enabled by computer-mediated communications and the distribution of sexually explicit materials on-line (DiMarco 2003; Wall 2001). Virtually all sexual fetishes and interests are represented in some way on the Internet, whether through forums, individually produced erotic fiction, images, and traditional forms of pornography (Comartin et al. 2013; DiMarco 2003; Quinn and Forsyth 2005). The anonymous nature of the Internet allows individuals to become part of virtual subcultures focused on activities that may not be accepted in the larger society and gain a sense of social support and validation (Robinson and Vidal-Ortiz 2013; Rosenmann and Safir 2006). For instance, there is now substantial evidence indicating that sex workers use the Internet as a means to advertise their services and solicit clients for real world meetings (Cunningham and Kendall 2010; Sharp and Earle 2003). At the same time, the clients of prostitutes use the Internet to discuss service providers and their experiences on- and off-line (Holt and Blevins 2007).

Cyber-porn and obscenity also includes the problems of pedophilia, where individuals seek out sexual or emotional relationships with children, and the production of child pornography (Jenkins 2001). Researchers have begun to explore the characteristics of child pornography users and sex offenders (Seigfried et al. 2008; Young 2008) as well as the way offenders use technology to access child victims through grooming techniques (Williams et al. 2013). The increased legislative and policing efforts applied to child pornography and sex offending have also led some researchers to explore the factors increasing the likelihood of arrest for child pornography possession (Wolak et al. 2004).

Finally, researchers have begun to explore the role of the Internet in facilitating social support networks and a subculture of pedophilia that engender sex offending (Durkin and Bryant 1999; Holt et al. 2010b; Jenkins 2001; Quayle and Taylor 2002). The Internet provides an anonymous mechanism for individuals to identify others who share their sexual proclivities that would not otherwise be possible in the real world (Holt et al. 2010b; Jenkins 2001). In turn, individuals can discuss their feelings about sexual attraction and emotional connections with children, particularly through the use of terms like ‘‘child love’’ to describe their attractions rather than pedophilia (Durkin and Bryant 1999; Holt et al. 2010b; Jenkins 2001). They also discuss sexual behaviors and fetishes as well as specific attractions, such as age ranges (Holt et al. 2010b; Jenkins 2001). Thus, these studies are vital to expand our knowledge of the problem of child sexual exploitation and victimization.

The research literature surrounding the use of the Internet for deviant sexual interests and activities has increased dramatically over the last two decades (DiMarco 2003; Quinn and Forsyth 2005). There are a number of qualitative studies assessing variations in the use of the Internet by groups interested in various sexual interests that are outside of societal norms. Researchers have recently explored the practices of individuals interested in beastiality (Durkin et al. 2006; Maratea 2011), bugchasing (Grov 2004; Tewksbury 2006), recording live streaming sex shows (Roberts and Hunt 2012), and various aspects of the BDSM subculture (Denney and Tewksbury 2013; Durkin 2007; Quinn and Forsyth 2005).

Not only do these studies help demonstrate the scope of sexual deviance occurring in on-line environments, but they also demonstrate the value of CMCs in the formation of deviant subcultures that support sexual fetishes and crimes, no matter how unusual (Quinn and Forsyth 2005; Rosenmann and Safir 2006). There is, however, a need for research exploring the applicability of criminological theories, such as social learning, to account for exposure to and involvement in the various sexual subcultures present on-line (see Quinn and Forsyth 2013 for summary).

A growing body of scholarship has also developed around the use of technology in support of the sex trade. Several studies have approached this issue from the client’s point of view using data from forums (Holt and Blevins 2007; Holt et al. 2008; Milrod and Weitzer 2012) and review sites (Sharp and Earle 2003). These studies demonstrate the value of the Internet as a tool to share information that would otherwise not be possible in the real world due to embarrassment or social stigma. These studies commonly assess the discussions between participants to understand how customers discuss the sex trade and the practices of customers and providers before, during, and after sex acts (Cunningham and Kendall 2010; Holt and Blevins 2007; Sharp and Earle 2003). In addition, research has demonstrated these forums’ impact on real and virtual displacement techniques to avoid law enforcement (Cunningham and Kendall 2010; Holt et al. 2008) and their value in communicating the negotiation processes of sexual encounters (Holt et al. 2008).

There is also a small, but growing, body of research examining the impact of the Internet on the sex trade from the provider’s perspective (Castle and Lee 2008; Milrod and Wietzer 2012). Pruitt and Krull (2011) recently performed a content analysis of ads for female escorts in the United States. The overwhelming majority of ads focus on the physical appearance of the provider, as well as the various services and experiences they offer to clients. Similarly, Davies and Evans (2007) utilized a series of posts from a website designed for British escorts to exchange information to explore the issue of violence during paid sexual encounters. The findings suggest that not only do escorts experience physical violence and must take steps to mitigate this risk, but they also face electronic harassment, which has no immediate resolution. Thus, additional research is needed to expand our understanding of the experience of sex workers during paid encounters.

There is also a small body of research on the phenomena of sex tourism, where individuals travel to foreign countries for the purpose of having sex with prostitutes and other sex workers. These studies generally utilize Web forums and advertisements from tourist websites in order to document the role of the Internet in facilitating tourist activities. They generally indicate actors learn how and where to travel, what to do when interacting with locals, the process of soliciting sexual services, and the expected costs for paid encounters, which may vary substantially based on personal experience (Chow-White 2006; DeCurtis 2003; Evans et al. 2000).

The generally exploratory nature of these studies is useful to demonstrate the utility and scope of the Internet for sexual services. Their use of primarily open source data sets, such as advertisements or forum posts, is invaluable to assess the discourse on the sex trade and refine the use of on-line data as a meaningful resource for social scientists. At the same time, they do not necessarily provide meaningful advancements for criminological theory or truly demonstrate the ways that technology differentially affects the behaviors of sex workers and clients. Furthermore, we know generally little about the experiences of both the clients and providers for homosexual acts and their use of the Internet to solicit services (Lee-Gonyea et al. 2009).

Taken as a whole, the research literature may benefit from studies that combine on-line data with surveys or in-depth interviews to improve and assess criminological and sociological theories. For instance, Cunningham and Kendall (2011) examined the frequency of posts in city-specific forums in and around major events, such as political conventions, to track variations in the ways that johns' communications patterns change as a result of real world events. These authors also utilized an on-line survey instrument with a population of prostitutes to measure the perceived risks and benefits of technology use in solicitation processes, as well as variations in technology use based on age and race (Cunningham and Kendall 2010). Similarly, Milrod and Monto (2012) surveyed participants in one of the larger escort review sites in the United States to refine the meaning of the Girlfriend Experience (GFE) and how much that affects the experience of paid sexual encounters. These studies provide meaningful examples for future study in order to improve our theoretical understanding of the sex trade through innovative methodological strategies.

Cyberviolence

The fourth and final category in Wall's (2001) cybercrime typology is cyber-violence, which includes the various ways that individuals can cause harm in real or virtual environments. Many researchers have begun to examine the use of the Internet to facilitate stalking, harassment, and bullying on-line (Bocij 2004; Holt and Bossler 2009). The increased use of cellular text messages, e-mail, and social networking sites like Facebook allow individuals to constantly communicate with others making it possible to threaten or harass an individual at all times, regardless of physical proximity (Bocij 2004; Hinduja and Patchin 2009). Estimates of on-line harassment and bullying appear to have increased across juvenile populations due to greater access to technology and the social importance placed on virtual communications (Bocij 2004; Hinduja and Patchin 2009; Holt and Bossler 2009).

Acts of cyberviolence include the use of technology in support of social unrest and prospective acts of terror (Wall 2001). In fact, political and social movements are increasingly promoting their ideologies through the Web and social media as they allow individuals to control their message, rather than depending on traditional media outlets for promotion (Weimann 2005). There is some evidence of nation-states and motivated individuals engaging in large-scale hacking attacks against political and military targets. Similarly, politically driven groups have also employed hacking techniques to engage in more serious strikes against governments and political organizations (Brenner 2008). As technology increasingly supports the critical infrastructure necessary for the day-to-day operations of a nation, the threat of cyberattacks has become more tangible and serious. Thus, there is a need for substantive research to understand how extremists, terror organizations, and lone wolf actors may engage in acts of cyberviolence.

The majority of research in the area of cyberviolence, however, focuses on acts of bullying, harassment, and stalking. Research assessing the prevalence of bullying and harassment on-line among youth populations has grown in the United States (Hinduja and Patchin 2009; Jones et al. 2012), Canada (Beran and Li 2005, 2007), Turkey (Erdur-Baker 2010), and various parts of Asia (Hokoda et al. 2006; Wong et al. 2008). Recent evidence from a multi-wave nationally representative sample of youth in the United States suggests that the prevalence of on-line harassment victimization has increased from 6% in 2000 to 11% in 2010 (Jones et al. 2012). This is lower than the rates of cyberbullying, with estimates generally between 30 to 35%, observed in convenience samples of youth (Marcum 2010; Hinduja and Patchin 2009). Similar variations are evident in reports of cyberstalking based on the operationalization of stalking, which range from 6.5% to over 30% in a nationally representative sample of college students (see Reyns et al. 2012).

In addition to illustrating that the rate of bullying victimization is growing, these studies have found significant correlates of on-line harassment and cyberbullying victimization. Specifically, females report a slightly higher prevalence of victimization (Bossler et al. 2012; Holt and Bossler 2009; Moore et al. 2010; Pelfrey and Weber 2013; Wolak et al. 2012) and are more likely to experience serious psychological consequences such as depression or suicidal ideation (Kim et al. 2005; Klomek et al. 2008). There are mixed findings, however, concerning racial differences in cyberbullying offending and victimization rates (Bossler et al. 2012; Moore et al. 2010; Pelfrey and Weber 2013; Wolak et al. 2012). Strong evidence suggests that poor educational performance is related to traditional bullying offending and victimization (Bossler et al. 2012; Glew et al. 2005; Hinduja and Patchin 2009).

A number of criminological theories have been examined to understand their value in understanding both cyberbullying and harassment. Patchin and Hinduja (2011) found limited evidence for general strain theory constructs (Agnew 2006), such as strain and negative emotions, in accounting for cyberbullying offending. Similarly, Hay and colleagues (2010) also found limited support for the experience of cyberbullying victimization as a source of strain that may predict self harm and suicidal ideation. There is also limited evidence that low self-control may affect individual willingness to engage in on-line harassment (Holt et al. 2012), although this is mediated by deviant peer associations.

A larger body of scholarship has developed testing the applicability of routine activity theory to account for harassment and bullying victimization. The evidence suggests that routine technology use has some effect on the risk of victimization, including spending time in chatrooms, social networking sites, and e-mail (Bossler et al. 2012; Hinduja and Patchin 2009; Holt and Bossler 2009; Moore et al. 2010; Ybarra et al. 2007). In addition, individual involvement in bullying, harassment, and other forms of cybercrime increase the risk of victimization (Holt and Bossler 2009; Holt et al. 2012; Hinduja and Patchin 2009; Ybarra et al. 2007). Similarly, peer involvement in offending increases the risk of victimization (Bossler et al. 2012; Hinduja and Patchin 2009; Holt and Bossler 2009). The value of guardianship measures, however, is mixed as protective programs like filtering software do little to reduce the risk of victimization (see Holt and Bossler 2009; Marcum 2010). In addition, Moore and colleagues (2010) found that parental regulation of Internet usage did not significantly affect on-line harassment victimization. Personal guardianship measures, such as computer skill, also appear to have a mixed impact on the risk of victimization (Bossler et al. 2012; Holt and Bossler 2009).

Scholars need to place more energy in evaluating the impact of the emerging anti-bullying legislation and administrative efforts to curb cyberbullying in schools (see Marcum 2010). States have also increasingly begun to adopt strategies to reduce the incidence of bullying outside of school grounds, particularly after high profile youth suicides. Kraft and Wang (2009) found that the most effective penalty as viewed by offenders themselves is the restriction of his or her Internet and technology use, a penalty implemented by parents, not schools. Thus, evaluations of cyberbullying and harassment programs that include parents are vital in understanding how best to decrease this problem. Similarly, there is a need for researchers to assess the factors that affect the likelihood of reporting bullying victimization to parents, teachers, and others in a position of power.

Although there is a growing body of research on cyberbullying, harassment, and stalking, generally little research on the phenomena of cyberterrorism and on-line extremism has been conducted. Although the term ''cyberterrorism'' varies country to country, it typically includes the use of the Internet as an attack vehicle or communications vehicle to incite fear in and harm a population of non-combatants (Britz 2010; Brenner 2008). To that end, several studies have examined the use of the Internet as a mechanism to distribute harmful materials, such as manuals on attack techniques (Weimann 2005), promote agendas to the general public, and possibly recruit (Freiburger and Crane 2008; Weimann 2005). Much less research explores the use of cyberattacks against various targets by extremist groups. One example is Jordan and Taylor's (2004) study in which they conducted interviews with a small number of hackers who were involved in hacks as a means to protest social and political policies.

Few researchers have employed survey methods to assess the value of criminological theories to account for involvement in acts of cyber-protest or terror. Recent research by Holt and Kilger (2012) utilized a scenario-based survey mechanism within a sample of college students to document their willingness to engage in protest activities and extremist behaviors on- and off-line. Although they found few correlates for willingness to engage in acts such as Web defacements and other forms of cyber-attack, one consistent predictor was a willingness to engage in activities in the real world. Thus, it may be that those who are likely to protest and engage in civil disobedience in one environment may do so in another (Holt and Kilger 2012). Further research utilizing demographically diverse samples could help to determine the influence of various attitudinal and behavioral factors on the willingness to engage in virtual and real acts of violence (Holt and Kilger 2012; Rege 2013).

A limited body of criminological scholarship assessing attacks against critical infrastructure and SCADA systems also exists (Brodscky and Radvanovsky 2011; Rege 2013). Rege (2013) argued for research examining the applicability of Situational Crime Prevention to SCADA system security. The technical knowledge required in order to work with SCADA systems requires individuals with an appreciation for both criminological theory and the technological issues affecting the hardware and software present in these systems. Additionally, there are few, if any, open source reporting bodies that provide statistics on attacks against these systems. The sensitive nature of critical infrastructure makes it difficult for vulnerabilities and attacks to be made known without compromising the security of these systems and of the nation in general.

Thus, future researchers will need access to sensitive data sources and industry experts in order to properly assess this hidden form of cybercrime.

IMPLICATIONS AND AVENUES FOR FUTURE RESEARCH

Over the last 20 years, there has been a substantial increase in the research literature on various forms of cybercrime. These studies have expanded our knowledge of the prevalence of cybercrime offending and victimization as well as the general influence of technology on various forms of offending behaviors. As a whole, these studies have generally demonstrated that traditional criminological theories and postulates apply in virtual environments. Thus, this supports Grabosky's (2001) supposition that cybercrimes may be ''old wine in new bottles.'' Specifically, offenders may adjust their tactics to fit new environments, but the general nature of criminality in on-line spaces has not changed.

Although we have highlighted specific theoretical and methodological issues that should be addressed within each of Wall's (2001) four-category cybercrime typology, there are several larger questions that must be considered. Specifically, researchers need to assess under-examined forms of cybercrime offending and victimization, especially involving malware, hacking, and fraud. In fact, some of these offenses now operate in tandem, combining elements of hacking and fraud in order to affect large populations (Chu et al. 2010; Holt and Lampke 2010; Motoyama et al. 2011). A small body of research from both computer scientists and criminologists has begun to examine this problem through the identification of on-line markets where cybercriminals buy and sell stolen data and information acquired through various sources (Chu et al., 2010; Holt and Lampke 2010; Motoyama et al. 2011). Regardless of the discipline, these studies indicate that stolen data markets facilitate the sale of credit card and bank account information, Personal Identification Numbers (PINs), and supporting customer information obtained from victims around the world in lots of tens or hundreds of accounts. Furthermore, most active stolen data markets currently operate primarily via websites hosted in foreign nations, whose users communicate in Russian characters rather than English (see Chu et al. 2010; Dunn 2012; Symantec Corporation 2012). Thus, qualitative and quantitative research is needed assessing the factors that shape these markets, the factors affecting the costs for data, and the network structures affecting participants. Such research would greatly expand our understanding of the nature of these offenses generally.

Finally, most cybercrime studies use components from traditional criminological theories, particularly routine activity theory, social learning, and the general theory of crime. Few cybercrime scholars have examined other criminological theories, such as lifecourse theories, within our field. The increasingly rapid adoption of technology at all ages in industrialized nations requires research identifying how the use of computers and the Internet affect adolescent development through adulthood and involvement in both on- and off-line offending. Such research could expand our knowledge of how the age–crime curve relates to virtual spaces. At the same time, there are a number of emerging theories that focus exclusively on cybercrimes, such as space-transition theory (Jaishankar 2008). This perspective argues that individuals engage in cybercrime due to the lack of deterrents, increased anonymity, and repressed desires to offend in the real world. Thus, the field needs to examine the breadth of existing and recent criminological theory in order to expand our knowledge of cybercrimes.

Scholars also need to research the law enforcement response to cybercrimes at the local, state, and federal levels (e.g., Stambaugh et al. 2001). The range of offenses enabled by technology requires unique investigative tools, training, and resources in order to fully investigate and clear cases. The jurisdictional issues evident also make it difficult for victims to know who may be responsible for the investigation of an offense. As a result, there is a need to understand how police agencies have adapted over time to respond to cybercrime calls for service. The current body of research primarily examines ways that police management perceives of these offenses (Hinduja 2004; Senjo 2004; Stambaugh et al. 2001), although a small number of studies explore these issues among line officers (Bossler and Holt 2012). These continuous changes require research exploring the awareness, perceptions, and preparation for dealing with cybercrimes from the vantage point of line officers and managers at all levels. These studies are pivotal to guide policy development to improve the resources available for law enforcement to increase their overall capabilities.

Finally, research is needed to understand how the larger criminal justice system is responding to cybercrimes at all levels. While cybercriminals may constitute a small proportion of the current population of individuals processed by the courts and correctional system, it is vital that researchers consider the sanctions they receive and the experiences of these actors. For instance, Smith and colleagues (2004) explored how three countries' court systems handled cybercrime cases and the various sentences cybercriminals received. Few, however, have attempted to replicate this study or document any changes in the number of actors processed at the state level for cybercrimes. Such research could greatly expand our knowledge of the ways that the criminal justice system has changed in response to the evolution of offending through technological means.

REFERENCES

Agnew, Robert. 2006. ''General Strain Theory: Current Status and Directions for Further Research.'' Pp. 137–158 in *Taking Stock: The Status of Criminological Theory (Advances in Criminological Theory, Vol. 16)*, edited by Francis T. Cullen John P. Wright, and Kristie R. Blevins. New Brunswick, NJ: Transaction.

Anderson, Jacqueline. 2010. ''Understanding the Changing Needs of the US Online Consumer, 2010. An Empowered Report: How Online and Mobile Behaviors are Changing.'' Forrester Research. Retrieved August 15, 2011 (http://www.forrester.com/rb/Research/understanding_changing_needs_of_us_on-line_consumer%2C/q/id/57861/t/2)

Bachmann, Michael. 2007. ''Lesson Spurned? Reactions of Online Music Pirates to Legal Prosecutions by the RIAA.'' *International Journal of Cyber Criminology* 2(1):213–227.

Beran, Tanya and Qing Li. 2005. ''Cyber-Harassment: A study of a New Method for an Old Behavior.'' *Journal of Educational Computing Research* 32:265–277.

———. 2007. ''The Relationship between Cyberbullying and School Bullying.'' *Journal of Student Wellbeing* 1:15–33.

Bocij, Paul. 2004. *Cyberstalking: Harassment in the Internet Age and How to Protect Your Family*. Westport, CT: Praeger.

Bossler, Adam M. and George W. Burruss. 2011. ''The General Theory of Crime and Computer Hacking: Low Self-Control Hackers?'' Pp. 38–67 in *Corporate Hacking and Technology Driven Crime: Social Dynamics and Implications*, edited by Thomas J. Holt and Bernadette H. Schell. Hershey, PA: IGI Global.

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

———. 2010. ''The Effect of Self Control on Victimization in the Cyberworld.'' *Journal of Criminal Justice* 38: 227–236.

———. 2012. ''Patrol Officers' Perceived Role in Responding to Cybercrime.'' *Policing: An International Journal of Police Strategies and Management* 35(1):165–181.

Bossler, Adam M., Thomas J. Holt, and David C. May. 2012. ''Predicting Online Harassment among a Juvenile Population.'' *Youth and Society* 44:500–523.

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

Britz, M. T. 2010. ''Terrorism and Technology: Operationalizing Cyberterrorism and Identifying Concepts.'' Pp. 193–220 in *Crime On-Line: Correlates, Causes, and Context*, edited by T. J. Holt. Raleigh, NC: Carolina Academic Press.

Brodscky, Jacob and Robert Radvanovsky. 2011. ''Control Systems Security.'' Pp. 187–204 in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by Thomas J. Holt and Bernadette H. Schell. Hershey, PA: IGI-Global.

Burruss, George W., Adam M. Bossler, and Thomas J. Holt. 2012. ''Assessing the Mediation of a Fuller Social Learning Model on Low Self-Control's Influence on Software Piracy.'' *Crime and Delinquency*. doi:10.1177/0011128 712437915.

Business Software Alliance. 2012. *Shadow Market: 2011 BSA Global Software Piracy Study*. Retrieved April 10, 2013 (http://globalstudy.bsa.org/2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf).

Castle, Tammy and Jenifer Lee. 2008. ''Ordering Sex in Cyberspace: A Content Analysis of Escort Websites.'' *International Journal of Cultural Studies* 11:107–121.

Choi, Kyung C. 2008. ''Computer Crime Victimization and Integrated Theory: An Empirical Assessment.'' *International Journal of Cyber Criminology* 2:308–333.

Chow-White, Peter A. 2006. ''Race, Gender, and Sex on the Net: Semantic Networks of Selling and Storytelling Sex Tourism.'' *Media, Culture, and Society* 28:883–905.

Chu, Bill, Thomas J. Holt, and Gail Joon Ahn. 2010. *Examining the Creation, Distribution, and Function of Malware On-Line*. Washington, DC: National Institute of Justice. NIJ Grant No. 2007-IJ-CX-0018.

Comartin, Erin, Roger Kernsmith, and Poco Kernsmith. 2013. '' 'Sexting' and Sex Offender Registration: Do Age, Gender, and Sexual Orientation Matter?'' *Deviant Behavior* 34(1):38–52.

Cunningham, Scott and Todd Kendall. 2010. ''Sex for Sale: Online Commerce in the World's Oldest Profession.'' Pp. 114–140 in *Crime On-line: Correlates, Causes, and Context*, edited by Thomas J. Holt. Raleigh, NC: Carolina Academic Press.

———. 2011. ''Men-in-Transit and Prostitution: Using Political Conventions as a Natural Experiment.'' *The B. E. Journal of Economic Analysis and Policy* 11:1–18.

Davies, Kim and Lorraine Evans. 2007. ''A Virtual View of Managing Violence among British Escorts.'' *Deviant Behavior* 28(6):525–551.

Decary-Hetu, David and Benoit Dupont. 2012. ''The Social Network of Hackers.'' *Global Crime* 13:160–175.

DeCurtis, Christina. 2003. ''Prostitution, Sex Tourism on the Internet: Whose Voice is Being Heard?'' *Computers and Society* 33:3–11.

Denney, Andrew S. and Richard Tewksbury. 2013. ''Characteristics of Successful Personal Ads in a BDSM On-Line Community.'' *Deviant Behavior* 34(2):153–168.

DiMarco, Heather. 2003. ''The Electronic Cloak: Secret Sexual Deviance in Cybersociety.'' Pp. 53–67 in *Dot.cons: Crime, Deviance, and Identity on the Internet*, edited by Yvonne Jewkes. Portland, OR: Willan Publishing.

Dunn, Jeff E. 2012. ''Russia Cybercrime Market Doubles in 2011, Says Report.'' *IT World Today*. Retrieved June 20, 2012 (http://www.itworld.com/security/272448/russia-cybercrime-market-doubles-2011-says-report).

Durkin, Keith F. 2007. ''Show Me the Money: Cybershrews and On-Line Money Masochists.'' *Deviant Behavior* 28:355–378.

Durkin, Keith F. and Clifton D. Bryant. 1999. ''Propagandizing Pederasty: A Thematic Analysis of the Online Exculpatory Accounts of Unrepentant Pedophiles.'' *Deviant Behavior* 20:103–127.

Durkin, Keith, Craig J. Forsyth, and James F. Quinn. 2006. ''Pathological Internet Communities: A New Direction for Sexual Deviance Research in a Post Modern Era.'' *Sociological Spectrum* 26:595–606.

Erdur-Baker, Odum. 2010. ''Cyberbullying and its Correlation to Traditional Bullying, Gender and Frequent Risky Usage of Internet-Mediated Communication Tools.'' *New Media Society* 12:109–125.

Evans, Rhonda D., Craig J. Forsyth, and George Woodell. 2000. ''Macro and Micro Views of Erotic Tourism.'' *Deviant Behavior* 21(6):537–550.

Freiburger, Tina and Jeffrey S. Crane. 2008. ''A Systematic Examination of Terrorist Use of the Internet.'' *International Journal of Cyber Criminology* 2(1):309–319.

Glew, Gwen M., Ming-Yu Fan, Wayne Katon, Frederick P. Rivara, and Mary A. Kernic. 2005. ‘‘Bullying, Psychosocial Adjustment, and Academic Performance in Elementary School.’’ *Archives of Pediatrics and Adolescent Medicine* 159:1026–1031.

Gordon, Sarah. 2000. ‘‘Virus Writers: The End of the Innocence?’’ Retrieved June 1, 2007 (http://www.research.ibm.com/antivirus/SciPapers/VB2000SG.pdf).

Gordon, Sarah and Ma Qingxiong. 2003. *Convergence of Virus Writers and Hackers: Fact or Fantasy?* Cupertine, CA: Symantec.

Gottfredson, Michael R. and Travis Hirschi. 1990. *A General Theory of Crime*. Stanford, CA: Stanford University Press.

Grabosky, Peter N. 2001. ‘‘Virtual Criminality: Old Wine in New Bottles?’’ *Social and Legal Studies* 10:243–249.

Grabosky, Peter, Russell G. Smith, and Gillian Dempsey. 2001. *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge, UK: Cambridge University Press.

Grov, Christian. 2004. ‘‘Make Me Your Death Slave: Men Who Have Sex with Men and Use the Internet to Intentionally Spread HIV.’’ *Deviant Behavior* 25:329–349.

Hay, Carter, Ryan C. Meldrum, and Karen Mann. 2010. ‘‘Traditional Bullying, Cyber Bullying, and Deviance: A General Strain Theory Approach.’’ *Journal of Contemporary Criminal Justice* 26:130–147.

Higgins, George E. 2005. ‘‘Can Low Self-Control Help with the Understanding of the Software Piracy Problem?’’ *Deviant Behavior* 26:1–24.

Higgins, George E. and Catherine D. Marcum. 2011. *Digital Piracy: An Integrated Theoretical Approach*. Raleigh, NC: Carolina Academic Press.

Higgins, George E., Brian D. Fell, and Abby L. Wilson. 2006. ‘‘Digital Piracy: Assessing the Contributions of an Integrated Self-Control Theory and Social Learning Theory Using Structural Equation Modeling.’’ *Criminal Justice Studies* 19:3–22.

Higgins, George E., Catherine D. Marcum, Tina L. Freiburger, and Melissa L. Ricketts. 2012. ‘‘Examining the Role of Peer Influence and Self-Control on Downloading Behavior.’’ *Deviant Behavior* 33(5):412–423.

Hinduja, Sameer. 2003. ‘‘Trends and Patterns among Software Pirates.’’ *Ethics and Information Technology* 5:49–61.

———. 2004. ‘‘Perceptions of Local and State Law Enforcement Concerning the Role of Computer Crime Investigative Teams.’’ *Policing: An International Journal of Police Strategies and Management* 27:341–357.

Hinduja, Sameer and Jason R. Ingram. 2008. ‘‘Self-Control and Ethical Beliefs on the Social Learning of Intellectual Property Theft.’’ *Western Criminology Review* 9:52–72.

Hinduja, Sameer and Justin W. Patchin. 2009. *Bullying beyond the Schoolyard: Preventing and Responding to Cyberbullying*. New York: Corwin Press.

Hokoda, Audrey, Hsuch-Huei Lu, and Manuel Angeles. 2006. ‘‘School Bullying in Taiwanese Adolescents.’’ *Journal of Emotional Abuse* 6:69–90.

Holt, Thomas J. 2007. ‘‘Subcultural Evolution? Examining the Influence of On-and Off-Line Experiences on Deviant Subcultures.’’ *Deviant Behavior* 28:171–198.

———. 2009. ‘‘Lone Hacks or Group Cracks: Examining the Social Organization of Computer Hackers.’’ Pp. 336–355 in *Crimes of the Internet*, edited by Frank Smalleger and Michael Pittaro. Upper Saddle River, NJ: Pearson Prentice Hall.

———. 2010. ‘‘Exploring Strategies for Qualitative Criminological and Criminal Justice Inquiry Using On-Line Data.’’ *Journal of Criminal Justice Education* 21:300–321.

Holt, Thomas J. and Adam M. Bossler. 2009. ‘‘Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization.’’ *Deviant Behavior* 30:1–25.

Holt, Thomas J. and Danielle C. Graves. 2007. ‘‘A Qualitative Analysis of Advanced Fee Fraud Schemes.’’ *The International Journal of Cyber-Criminology* 1:137–154.

Holt, Thomas J. and Eric Lampke. 2010. ‘‘Exploring Stolen Data Markets On-Line: Products and Market Forces.’’ *Criminal Justice Studies* 23:33–50.

Holt, Thomas J. and Heith Copes. 2010. ‘‘Transferring Subcultural Knowledge On-line: Practices and Beliefs of Persistent Digital Pirates.’’ *Deviant Behavior* 31:625–654.

Holt, Thomas J. and Kristie R. Blevins. 2007. ‘‘Examining Sex Work from the Client’s Perspective: Assessing Johns Using Online Data.’’ *Deviant Behavior* 28:333–354.

Holt, Thomas J. and Max Kilger. 2008. ‘‘Techcrafters and Makecrafters: A Comparison of Two Populations of Hackers.’’ WOMBAT Workshop on Information Security Threats Data Collection and Sharing, Amsterdam, Holland.

———. 2012. ‘‘Examining Willingness to Attack Critical Infrastructure On and Off-Line.’’ *Crime and Delinquency* 58(5):798–822.

Holt, Thomas J. and Michael G. Turner. 2012. ‘‘Examining Risks and Protective Factors of On Line Identity Theft.’’ *Deviant Behavior* 33:308–323.

Holt, Thomas J., Adam M. Bossler, and David C. May. 2012. ‘‘Low Self-Control Deviant Peer Associations and Juvenile Cyberdeviance.’’ *American Journal of Criminal Justice* 37(3):378–395.

Holt, Thomas J., George W. Burruss, and Adam M. Bossler. 2010a. ‘‘Social Learning and Cyber Deviance: Examining the Importance of a Full Social Learning Model in the Virtual World.’’ *Journal of Crime and Justice* 33:15–30.

Holt, Thomas J., Kristie R. Blevins, and Joseph B. Kuhns. 2008. ‘‘Examining the Displacement Practices of Johns with On-Line Data.’’ *Journal of Criminal Justice* 36:522–528.

Holt, Thomas J., Kristie R. Blevins, and Natasha Burkert. 2010b. ‘‘Considering the Pedophile Subculture On-Line.’’ *Sexual Abuse: Journal of Research and Treatment* 22:3–24.

Holtfreter, Kristy, Michael D. Reisig, and Travis C. Pratt. 2008. ‘‘Low Self-Control, Routine Activities, and Fraud Victimization.’’ *Criminology* 46:189–220.

Huang, Wilson and Andrea Brockman. 2010. ‘‘Social Engineering Exploitations in Online Communications Examining Persuasions Used in Fraudulent Emails.’’ Pp. 87–111 in *Crime On-Line: Correlates, Causes and Context*, edited by Thomas J. Holt. Durham, NC: Carolina Academic Press.

Ingram, Jason R. and Sameer Hinduja. 2008. ‘‘Neutralizing Music Piracy: An Empirical Examination.’’ *Deviant Behavior* 29:334–366.

Internet Crime Complaint Center (IC3). 2012. ‘‘2011 Internet Crime Report.’’ Retrieved April 5, 2013 (http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf)

Jaishankar, K. 2008. ‘‘Space Transition Theory of Cyber Crimes.’’ Pp. 283–301 in *Crimes of the Internet*, edited by Frank Schmalleger and Michael Pittaro. Upper Saddle River, NJ: Prentice Hall.

James, Lance. 2005. *Phishing Exposed*. Rockland, MA: Syngress.

Jenkins, Paul. 2001. *Beyond Tolerance: Child Pornography on the Internet*. New York: New York University Press.

Jones, Lisa M., Kimberly J. Mitchell, and David Finkelhor. 2012. ‘‘Trends in Youth Internet Victimization: Findings from Three Youth Internet Safety Surveys 2000–2010.’’ *Journal of Adolescent Health* 50:179–186.

Jordan, Tim and Paul Taylor. 1998. ‘‘A Sociology of Hackers.’’ *The Sociological Review* 46:757–780.

———. 2004. *Hacktivism and Cyber Wars*. London: Routledge.

Kim, Young Shin, Yun-Joo Koh, and Bennett Leventhal. 2005. ‘‘School Bullying and Suicidal Risk in Korean Middle School Students.’’ *Pediatrics* 115:357–363.

King, Adam and Jim Thomas. 2009. ‘‘You Can’t Cheat an Honest Man: Making ($$$s and) Sense of the Nigerian E-Mail Scams.’’ Pp. 206–224 in *Crimes of the Internet*, edited by Frank Schmalleger and Michael Pittaro. Saddle River, NJ: Prentice Hall.

Klomek, Anat B., Andre Sourander, Kirsti Kumpulainen, Jorma Piha, Tuula Tamminen, Irma Moilanen, Fredrik Almqvist, and Madelyn S. Gould. 2008. ‘‘Childhood Bullying as a Risk for Later Depression and Suicidal Ideation among Finnish Males.’’ *Journal of Affective Disorders* 109:47–55.

Kraft, Ellen M. and Jinchang Wang. 2009. ‘‘Effectiveness of Cyber Bullying Prevention Strategies: A Study on Students’ Perspectives.’’ *International Journal of Cyber Criminology* 3(2):513–535.

Lee-Gonyea, Jenifer A., Tammy Castle, and Nathan E. Gonyea. 2009. ‘‘Laid to Order: Male Escorts Advertising on the Internet.’’ *Deviant Behavior* 30:321–348.

Maratea, Richard J. 2011. ‘‘Screwing the Pooch: Legitimizing Accounts in a Zoophilia On-Line Community.’’ *Deviant Behavior* 32(10):918–943.

Marcum, Catherine D. 2010. ‘‘Examining Cyberstalking and Bullying: Causes, Context, and Control.’’ Pp. 175–192 in *Crime On-Line: Correlates, Causes, and Context*, edited by Thomas J. Holt. Raleigh, NC: Carolina Academic Press.

Milrod, Christine and Martin A. Monto. 2012. ‘‘The Hobbyist and the Girlfriend Experience: Behaviors and Preferences of Male Customers of Internet Sexual Service Providers.’’ *Deviant Behaviors* 33(10):792–810.

Milrod, Christine and Ronald Weitzer. 2012. ‘‘The Intimacy Prism: Emotion Management among the Clients of Escorts.’’ *Men and Masculinities* 15(5):447–467.

Moore, Robert, Naga Tarun Guntupalli, and Tina Lee. 2010. ‘‘Parental Regulation and Online Activities: Examining Factors That Influence a Youth’s Potential to Become a Victim of Online Harassment.’’ *International Journal of Cyber Criminology* 4:685–698.

Motoyama, Marti, Damon McCoy, Kirill Levchenko, Stefan Savage, and Geoffrey M. Voelker. 2011. ‘‘An Analysis of Underground Forums.’’ *2011 Internet Measurement Conference*, 71–79.

National White Collar Crime Center (NWC3). 2010. ''Advance Fee Fraud: New Twists on an Old Scam.'' NW3C Research Brief, September 2010. Retrieved April 6, 2013 (http://www.nw3c.org/docs/whitepapers/advance_fee_fraud_september_201002E40E1D11A1.pdf?sfvrsn=9)

Newman, Grame and Ronald Clarke. 2003. *Superhighway Robbery: Preventing E-Commerce Crime*. Cullompton, UK: Willan Press.

Ngo, Fawn T. and Raymond Paternoster. 2011. ''Cybercrime Victimization: An Examination of Individual- and Situational-Level Factors.'' *International Journal of Cyber Criminology* 5:773–793.

Nhan, Johnny. 2013. ''The Evolution of Online Piracy: Challenge and Response.'' Pp. 61–80 in *Crime On-Line: Causes, Correlates, and Context,* 2nd ed., edited by Thomas J. Holt. Raleigh, NC: Carolina Academic Press.

PandaLabs. 2007. ''Malware Infections in Protected Systems.'' Retrieved February 20, 2008 (http://research.pandasecurity.com/blogs/images/wp_pb_malware_infections_in_protected_systems.pdf).

Patchin, Justin W. and Sameer Hinduja. 2011. ''Traditional and Nontraditional Bullying among Youth: A Test of General Strain Theory.'' *Youth and Society* 43:727–751.

Pelfrey, Jr., William V. and Nicole L. Weber. 2013. ''Keyboard Gangsters: Analysis of Incidence and Correlates of Cyberbullying in a Large Urban Student Population.'' *Deviant Behavior* 34(1):68–84.

Pew Internet and American Life. 2005. ''Pew Internet and American Life Project.'' Retrieved November 7, 2007 (http://www.pewinternet.org/Reports/2009/10_Home_Broadband_Adoption-2009.aspx).

Pratt, Travis C. and Francis T. Cullen. 2000. ''The Empirical Status of Gottfredson and Hirschi's General Theory of Crime: A Meta-Analysis.'' *Criminology* 38:931–964.

Pratt, Travis C., Kristie Holtfreter, and Matthew D. Reisig. 2010. ''Routine On-line Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory.'' *Journal of Research in Crime and Delinquency* 47:267–296.

Pratt, Travis C., Francis T. Cullen, Christine S. Sellers, Thomas Winfree, Tamara D. Madensen, Leah E. Daigle, Noelle E. Fearn, and Jacinta M. Gau. 2009. ''The Empirical Status of Social Learning Theory: A Meta-Analysis.'' *Justice Quarterly* 27:765–802.

Pruitt, Matthew and Amy Krull. 2011. ''Escort Advertisements and Male Patronage of Prostitutes.'' *Deviant Behavior* 32:38–63.

Quayle, Ethel and Max Taylor. 2002. ''Child Pornography and the Internet: Perpetuating a Cycle of Abuse.'' *Deviant Behavior* 23:331–361.

Quinn, James F. and Craig J. Forsyth. 2005. ''Describing Sexual Behavior in the Era of the Internet: A Typology for Empirical Research.'' *Deviant Behavior* 26:191–207.

———. 2013. ''Red Light Districts on Blue Screens: A Typology for Understanding the Evolution of Deviant Communities on the Internet.'' *Deviant Behavior* 34:579–585.

Rege, Aunshul. 2013. ''Industrial Control Systems and Cybercrime.'' Pp. 191–218 in *Crime On-line: Causes, Correlates, and Context*, 2nd ed., edited by Thomas J. Holt. Raleigh, NC: Carolina Academic Press.

Reyns, Bradford W., Billy Henson, and Bonnie S. Fisher. 2012. ''Stalking in the Twilight Zone: Extent of Cyberstalking Victimization and Offending among College Students.'' *Deviant Behavior* 33:1–25.

Roberts, Joshua W. and Scott A. Hunt. 2012. ''Social Control in a Sexually Deviant Cybercommunity: A Cappers' Code of Conduct.'' *Deviant Behavior* 33(10):757–773.

Robinson, Brandon Andrew and Salvador Vidal-Ortiz. 2013. ''Displacing the Dominant 'Down Low' Discourse: Deviance, Same-Sex Desire, and Craigslist.org.'' *Deviant Behavior* 34(3):224–241.

Rogers, Marcus, Natalie D. Smoak, and Jia Liu. 2006. ''Self-Reported Deviant Computer Behavior: A Big-5 Moral Choice, and Manipulative Exploitive Behavior Analysis.'' *Deviant Behavior* 27:245–268.

Rosenmann, Amir and Marylin P. Safir. 2006. ''Forced Online: Pushed Factors of Internet Sexuality: A Preliminary Study of Paraphilic Empowerment.'' *Journal of Homosexuality* 51:71–92.

Schell, Bernadette H. and John L. Dodge. 2002. *The Hacking of America: Who's Doing it, Why, and How*. Westport, CT: Quorum Books.

Seigfried, Katherine C., Richard W. Lovely, and Marcus K. Rogers. 2008. ''Self-Reported Online Child Pornography Behavior: A Psychological Analysis.'' *International Journal of Cyber Criminology* 2(1):286–297.

Senjo, Scott R. 2004. ''An Analysis of Computer-Related Crime: Comparing Police Officer Perceptions with Empirical Data.'' *Security Journal* 17:55–71.

Sharp, Keith and Sarah Earle. 2003. ''Cyberpunters and Cyberwhores: Prostitution on the Internet.'' Pp. 33–89 in *Dot Cons. Crime, Deviance and Identity on the Internet*, edited by Yvonne Jewkes. Portland, OR: Willan Publishing.

Siwek, Stephen E. 2007. ‘‘The True Cost of Sound Recording Piracy to the U.S. Economy.’’ *Institute for Policy Innovation Policy Report 188*. Retrieved April 1, 2013 (http://ipi.org/IPI/IPIPublications.nsf/PublicationLookup FullTextPDF/51CC65A1D4779E408625733E00529174/$File/SoundRecordingPiracy.pdf?OpenElement).

Skinner, William F. and Anne F. Fream. 1997. ‘‘A Social Learning Theory Analysis of Computer Crime among College Students.’’ *Journal of Research in Crime and Delinquency* 34:495–518.

Smith, Russell G., Peter Grabosky, and Gregor Urbas. 2004. *Cyber Criminals on Trial*. Cambridge, UK: Cambridge University Press.

Socialbakers. 2011. *United States Facebook Statistics*. Retrieved June 1, 2011 (http://www.socialbakers.com/facebook-statistics/united-states).

Stambaugh, Hollis, David S. Beaupre, David J. Icove, Richard Baker, Wayne Cassady, and Wayne P. Williams. 2001. *Electronic Crime Needs Assessment for State and Local Law Enforcement, National Institute of Justice*. Washington, DC: NCJ 186276.

Steinmetz, Kevin F. and Kenneth D. Tunnell. 2013. ‘‘Under the Pixelated Jolly Roger: A Study of On-Line Pirates.’’ *Deviant Behavior* 34:53–67.

Symantec Corporation. 2012. ‘‘Symantec Internet Security Threat Report, Volume 17.’’ Retrieved June 23, 2012 (http://www.symantec.com/threatreport/).

Taylor, Paul. 1999. *Hackers: Crime in the Digital Sublime*. London: Routledge.

Taylor, Robert W., Eric J. Fritsch, Jeff Liederbach, and Thomas J. Holt. 2010. *Digital Crime and Digital Terrorism*. 2nd ed. Upper Saddle River, NJ: Pearson Prentice Hall.

Tewksbury, Richard. 2006. ‘‘Click Here for HIV: An Analysis of Internet-Based Bug Chasers and Bug Givers.’’ *Deviant Behavior* 27:379–395.

The Numbers Guy. 2013. ‘‘Studios Struggle for Focus on Film Pirates’ Booty.’’ *The Wall Street Journal, April 5, 2013*. Retrieved April 13, 2013 (http://on-line.wsj.com/article/SB10001424127887324600704578402850894445768.html).

Turner, Sarah, Heith Copes, Kent R. Kerley, and Gary Warner. 2013. ‘‘Understanding On-line Work-At-Home Scams through an Analysis of Electronic Mail and Websites.’’ Pp. 81–108 in *Crime On-Line: Causes, Correlates, and Context*, 2nd ed., edited by Thomas J. Holt. Raleigh, NC: Carolina Academic Press.

Verini, James. 2010. ‘‘The Great Cyberheist.’’ *The New York Times*, November 14, 2010. Retrieved November 15, 2010 (http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html?_r=1).

Verison. 2012. ‘‘2012 Data Breach Investigations Report and Executive Summary.’’ Retrieved August 10, 2012 (http://www.verisionbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf)

Wall, David S. 2001. ‘‘Cybercrimes and the Internet.’’ Pp. 1–17 in *Crime and the Internet*, edited by David S. Wall. New York: Routledge.

———. 2007. *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge, UK: Polity Press.

Weimann, Gabriel. 2005. ‘‘How Modern Terrorism Uses the Internet.’’ *The Journal of International Security Affairs* 8:91–105.

Williams, Rebecca, Ian A. Elliott, and Anthony R. Beech. 2013. ‘‘Identifying Sexual Grooming Themes Used by Internet Sex Offenders.’’ *Deviant Behavior* 34:135–152.

Wolak, Janice, David Finkelhor, and Kimberly Mitchell. 2004. ‘‘Internet-Initiated Sex Crimes against Minors: Implications for Prevention Based on Findings from a National Study.’’ *Journal of Adolescent Health* 35:424.e11–424.20.

———. 2012. *Trends in Law Enforcement Responses to Technology-Facilitated Child Sexual Exploitation Crimes: The Third National Juvenile On-line Victimization Study (NJOV-3)*. Durham, NH: Crimes against Children Research Center.

Wolfe, Scott E., George E. Higgins, and Catherine D. Marcum. 2007. ‘‘Deterrence and Digital Piracy: A Preliminary Examination of the Role of Viruses.’’ *Social Science Computer Review* 26:317–333.

Wong, Dennis S. W., David P. P. Lok, T. Wing Lo, and Stephen K. Ma. 2008. ‘‘School Bullying among Hong Kong Chinese Primary Schoolchildren.’’ *Youth and Society* 40:35–54.

Yar, Majid. 2005. ‘‘The Novelty of Cybercrime.’’ *European Journal of Criminology* 2:407–427.

Ybarra, Michele L., Kimberly J. Mitchell, David Finkelhor, and Janis Wolak. 2007. ‘‘Internet Prevention Messages: Targeting the Right Online Behaviors.’’ *Archives of Pediatrics and Adolescent Medicine* 161:138–145.

Young, Kimberly. 2008. ‘‘Understanding Sexually Deviant Online Behavior from an Addiction Perspective.’’ *International Journal of Cyber Criminology* 2(1):298–307.

THOMAS J. HOLT is an Associate Professor in the School of Criminal Justice at Michigan State University whose research focuses on computer hacking, malware, and the role of the Internet in facilitating all manner of crime and deviance. He received his Ph.D. in criminology and criminal justice from the University of Missouri–Saint Louis in 2005. His work has been published in various journals including *Crime and Delinquency, Deviant Behavior*, the *Journal of Criminal Justice*, and *Youth and Society*.

ADAM M. BOSSLER is an Associate Professor of Criminal Justice and Criminology at Georgia Southern University. He earned his doctorate in criminology and criminal justice from the University of Missouri–St. Louis. His research focuses on examining the application of traditional criminological theories to cybercrime offending and victimization, how law enforcement responds to cybercrime, and exploring innovative correctional programs. His most recent publications can be found in *Crime & Delinquency, Youth & Society, American Journal of Criminal Justice, Policing*, and *Journal of Criminal Justice*.