ANNUAL REVIEWS

Annual Review of Criminology

Cyber-Dependent Crimes: An Interdisciplinary Review

David Maimon[1] and Eric R. Louderback[2]

[1]Department of Criminal Justice and Criminology, Georgia State University, Atlanta, Georgia 30303, USA; email: dmaimon@gsu.edu

[2]Department of Sociology, University of Miami, Coral Gables, Florida 33146, USA

Annu. Rev. Criminol. 2019. 2:191–216

First published as a Review in Advance on October 12, 2018

The *Annual Review of Criminology* is online at criminol.annualreviews.org

https://doi.org/10.1146/annurev-criminol-032317-092057

Copyright © 2019 by Annual Reviews. All rights reserved

ANNUAL REVIEWS CONNECT

www.annualreviews.org

- Download figures
- Navigate cited references
- Keyword search
- Explore related articles
- Share via email or social media

Keywords

cybercrime, cyber-dependent crimes, cyber-victimization, cyber-offending, hacking, situational crime prevention

Abstract

Online crime has increased in severity and frequency over the past two decades. However, although several scientific disciplines have commonly employed criminological theories to explain this phenomenon, mainstream criminology has devoted relatively scant attention to the investigation of cyber-criminals and their victims. Drawing on this assumption that more criminological attention should be given to this important type of crime, this article presents an interdisciplinary review of the current state of research on cyber-dependent crimes (i.e., crimes that require the use of computer technology to exist, such as hacking). We begin with a brief discussion of the ecosystem of cyber-dependent crimes and the key actors who operate within it, including the online offenders and enablers, targets and victims, and guardians. Next, we review empirical scholarship that pertains to each actor while distinguishing between nontheoretical research and theoretically driven studies. We then detail methodological and theoretical avenues that should be pursued by future research and discuss why criminological research should lead policy initiatives and guide the design of technical tools that improve the scientific community's ability to generate a safer and more secure cyber-environment. We conclude by discussing potential ways in which cyber-dependent crime research could pave the way for the advancement of mainstream criminological theory and research.

INTRODUCTION

Violent and property crime rates have been steadily decreasing since the early 1990s in the United States (FBI 2016, Zimring 2006) and around the globe (Tseloni et al. 2010). In contrast, the amount of cyber-dependent crimes,[1] i.e., illegal activities that can only be performed using a computer, computer networks, or other forms of information communication technology (Furnell et al. 2015, McGuire & Dowling 2013), increased consistently during the past two decades (Rantala 2008, FBI 2017). A recent report by the Center for Strategic and International Studies (Lewis 2018) indicates that Internet service providers (ISPs) record an average of 80 billion daily automated scans made by online cyber-criminals and aimed at identifying vulnerable targets. Data available from the Privacy Rights Clearinghouse suggest that these scanning efforts resulted in the loss of 4.8 billion records in 2016, with hacking incidents responsible for the loss of 60% of these records (PRCH 2017). Furthermore, users of private computers, smartphones, and even medical devices increasingly report infiltration of their devices by illegitimate users (Storm 2015). Still, despite the soaring estimated costs and prevalence of cyber-dependent crimes, as well as the increased attention devoted to criminological theories by information scientists, computer scientists, and cybersecurity experts in an effort to better understand these crimes, only a limited number of criminological studies on cybercrime have been published in top-tier criminological journals during the past 15 years (Bossler 2017).

Reflecting upon the driving forces behind the dearth of cyber-dependent crime research in major criminological outlets, Diamond & Bachmann (2015) suggested that criminologists' unfamiliarity with Internet technology and the cyber-environment, along with vague understandings of the full extent of these crimes' social implications, are two key reasons behind the marginalization of cybercrime research by mainstream criminology. This review is a unique opportunity to bring cybercrime research to the forefront of the criminological discipline by introducing the criminological community to the most recent cutting-edge research published on cyber-dependent crime by criminologists, information scientists, and cybersecurity scholars during the past 20 years. In addition to shedding light on the ecosystem of cyber-dependent crime and its key actors, we aim to draw on past research and highlight directions for future theoretical and policy-relevant contributions.

Importantly, in the past ten years, at least three relevant review articles have highlighted the state of and gaps in cybercrime research (Bossler 2017, D'Arcy & Herath 2011, Holt & Bossler 2014). Two of those reviews provide an assessment of the criminological scholarship around a wide range of both cyber-dependent and cyber-enabled crimes (i.e., all those offenses in which computers are used in a supporting capacity). In contrast, D'Arcy & Herath (2011) examined published research on the effectiveness of sanctions and organizational policies in deterring computer misconduct among employees. The current work moves beyond those previous reviews by (*a*) focusing only on research illuminating different junctures of the cyber-dependent crime ecosystem and (*b*) incorporating interdisciplinary evidence from studies published in criminological, computer science, information security, and cybersecurity outlets, as well as those that empirically tested criminological theories in cyberspace. We opted to keep this review focused on cyber-dependent crime research because such an approach allows us to highlight a set of illegal activities and actors that are less familiar in the criminological literature (unlike cyber-fraudsters, juvenile delinquents, and bullies) but still deserve criminological attention.

To lay the groundwork for the average reader who may not be familiar with cybercrime research and terminology, this piece starts with a brief review of the cybercrime ecosystem that supports

[1] In some literature, cyber-dependent crimes are also known as computer-focused crimes (Furnell 2002, Yar 2005).

the development of cyber-dependent crimes. We then discuss scientific evidence reflecting the current state of knowledge around the key actors that drive this phenomenon: online offenders and enablers, targets and victims, and guardians. For each of these actors, we highlight the major theoretical perspectives that have guided research efforts in the area and then propose directions for future research. Reflecting upon the potential impact of cyber-dependent crime research on the general criminological community, we conclude this piece by suggesting that continued criminological attention to cyber-dependent crimes could support the criminological community's efforts to go beyond analyses of offenders' motivations to include insights on all parts of the etiology of crime, including the interaction between criminal event participants, the unfolding of criminal events, and the settings in which these events occur (Meier et al. 2001, Short 1998). Furthermore, we conclude that the pursuit of criminological research on cyber-dependent crimes is vital for guiding the design of future cyber-environments (Lessig 2009) and for assessing regulations and controls that aim to improve cybersecurity (NIST 2014).

THE ECOSYSTEM OF CYBER-DEPENDENT CRIMES

An ecosystem is defined by biologists as the interacting biotic community and its environment (Dunlap & Catton 1979). Importing this concept to human societies, Duncan (1961) proposed that human populations employ social organization and technology in their efforts to adapt to the environment (either natural or built) and evolve. Drawing on these claims, several scholars suggested that the interactions among cyber-criminals, enablers (i.e., individuals who support the online criminal operations) (Moore et al. 2009), targets, and guardians (i.e., official law enforcement agencies and system administrators) (Grabosky 2016) form a unique ecosystem in which the activities of each actor influence the behaviors of other actors (Moore et al. 2009, Kraemer-Mbula et al. 2013). One important illegitimate activity that regulates the interaction between different actors in the cybercrime ecosystem is hacking.

Hacking or cracking is commonly defined as the unauthorized access of a computer system with criminal intention (Grabosky 2016). Similarly, cyber-trespassing is defined as the crossing of invisible boundaries of online environments (Wall 2001). Although one may contend that these terms are largely interchangeable and could be easily applied to describe system-trespassing events that require either low or high levels of technical sophistication (e.g., password guessing versus developing an attack tool), we believe that the term hacking may be interpreted to include a variety of behaviors, such as redesigning the configuration of hardware or software systems to alter their intended function (Bachmann 2010), as well as participation in the broader hacker subculture (Holt 2007, Steinmetz 2015), and therefore opt to use this term in our review.

A successful act of hacking requires an offender's engagement in a series of consecutive activities (Dey et al. 2012, Hartley 2015, Holt & Bossler 2016, Marcum et al. 2014, Steinmetz 2015, Young et al. 2007). During the initial phase of the event, the hacker performs a preliminary investigation of potential targets' social and technical vulnerabilities and gathers intelligence from both online (e.g., by browsing public websites and online resources) and offline environments (e.g., by looking over targets' shoulders on their computer screens). During the second stage, the hacker takes advantage of hardware and software vulnerabilities that were found in the initial reconnaissance stage and infiltrates the target asset (e.g., computer device or email account). Hackers may use malicious software like computer viruses and worms to exploit these vulnerabilities (Hughes & DeLone 2007, Wolfe et al. 2008). This software could be either developed by the attacking hacker or (more commonly) purchased online from malware writers who post their products on hacker forums and message boards. In the third stage, hackers elevate their privileges in the attacked asset and grant themselves permission to edit, create, and delete all available content in it. The

hacker may then install different types of malware that ensure easy access to the attacked asset, can harvest sensitive data (e.g., passwords, social security numbers, credit card numbers, and bank and email accounts) (Holz et al. 2009), provide remote control over the system (Waldrop 2016), and even deny access to the attacked system and the files it hosts (Luo & Liao 2009). In the final phase, hackers take steps to cover up the evidence of the hack by restoring the attacked asset back to its preattack state. Hackers report that their emotional experiences during the progression of a hacking event vary from frustration and boredom to happiness and that with the completion of a hack they feel pleasure and euphoria (Steinmetz 2015).

Hacking is considered by many as the point from which most types of cyber-dependent crimes begin. Specifically, gaining illegitimate access to computers allows hackers to launch website defacement, interfere with the lawful use of computers, and spread malicious software (Grabosky 2016).[2] Hackers' remote access to large numbers of illegitimately infiltrated assets provides fertile ground for the development of botnets, which are a collection of computer systems that receive commands remotely from the hackers that control them (Kremling & Parker 2017). These botnets allow their owners (bot herders) to launch two additional types of cyber-dependent crimes: spamming and distributed denial of service (DDoS) attacks. Spamming is the act of sending mass mailings. A DDoS attack is an intentional attempt to overwhelm a targeted computer system (usually one owned by a governmental agency or a commercial entity) with page views and users (i.e., traffic) such that the system becomes unavailable to legitimate users (Karami et al. 2016). DDoS attacks can distort the entire Internet communication of a target country, and the costs due to loss of business and IT expenditures are substantial independent of the company's size (Overvest & Straathof 2015).

Acknowledging the potential risks posed by cyber-dependent crimes to governments, businesses, and individual Internet users, cybersecurity experts have devoted considerable attention to developing tools and policies designed to prevent these crimes from developing (Waldrop 2016). However, to overcome the challenges posed by information technology and security experts' efforts to protect targets, a division of labor has evolved around hacking (Broadhurst et al. 2014). Enterprising individuals who possess specialized knowledge in programming (e.g., programmers who write malware), marketing (e.g., vendors who sell stolen data), and technology (e.g., technicians who support servers and computers) started developing specialized tools and platforms that automate many hacking activities, and they offer these tools for sale on online markets (Holt 2017). Today, these online markets allow cyber-dependent crime offenders and enablers to interact with each other, buy and sell malicious software and stolen data, lease botnet infrastructures to interested parties, and offer cybercrime as a service. These markets also attract the attention of law enforcement agencies and security professionals (i.e., guardians), who seek to infiltrate them, gather intelligence on offenders and the tools and data they are selling, and, in some instances, eventually shut them down (Chen et al. 2012, Glenny 2011).

CYBER-DEPENDENT CRIME OFFENDERS AND ENABLERS

The online environments that support the convergences of cyber-criminals, enablers, targets, and guardians exist on the surface web (which contains all the websites and computers that

[2]Importantly, hacking is also the starting point for the development of cyber-enabled crimes like data theft, espionage, unauthorized public disclosure of information, and click fraud (i.e., the practice of clicking on online ads with the intention of either increasing host website revenue or preventing advertiser revenue) (Wilbur & Zhu 2009).

are accessible to anyone with an Internet connection) and the deep web (which is up to 500 times larger than the surface web and consists of websites that are not searchable, business intranets, and medical databases) (Kremling & Parker 2017). Dark nets (also known as the dark web) form a subset of the deep web. Because of the extended anonymity that they provide, dark nets provide an attractive online platform for the development of networks and allegiances between criminals and enablers as well as for the initiation and development of illegal activities.

Cyber-Dependent Crime Offenders

A hacker is a person who uses computers to gain unauthorized access to other people's computer systems, networks, and data (Schell & Dodge 2002). Hackers' motivations to engage in hacking may include prestige, recreation, ideology, revenge, and profit, and their skill levels vary from very low to very high (Seebruck 2015). Several studies reveal that most cyber-dependent criminals have relatively low technical capability (NCA 2016). In fact, reports from college samples indicate that 10%–15% of individuals who engage in hacking activities are involved in password guessing, which is considered a low level of hacking (Bossler & Burruss 2011, Skinner & Fream 1997), whereas less than 5% engage in sophisticated attacks (Holt & Bossler 2014). In addition to classifying hackers based on their technical skill level, scholars have classified hackers based on their intent (e.g., white hat hackers who work for the good of system security versus black hat hackers who infiltrate systems in an unauthorized and malicious manner) (Furnell 2002) and their access to targets (e.g., insider hackers are legitimate users of a computer or network who misuse their privileges to access data they are not authorized to access, whereas outsider hackers are unauthorized users of the system) (Wall 2013). Several studies reported that hackers tend to be curious, creative and unconventional, and self-learners, and they possess problem-solving orientations, engage in systematic and technical thinking (Rogers 2006, Steinmetz 2015), and seek variety in the targets they attack (Ooi et al. 2012).

Hackers begin to infiltrate cyber-assets by themselves (Valnour 2009) and mainly hack alone. However, prior research suggests that hackers develop relationships with other hackers (in both online and offline environments) fairly early in their hacking careers (Schell & Dodge 2002). Reviewing the organizational structure of known cyber-offender groups, McGuire (2012) differentiated between disorganized groups of cyber-dependent offenders that mainly operate in online environments yet have no clear chain of command (i.e., a swarm structure) and organized groups with clear leadership and command structure (i.e., a hub structure). In addition to maintaining small, intimate peer networks, hackers may also be part of a broader community of hackers that utilize web forums to communicate and exchange knowledge, information, and tools (Macdonald & Frank 2017). These communication platforms are hosted mainly on the deep web and support the vitality of a subculture that emphasizes its members' knowledge of technology and demonstration of computer skill mastery (Holt & Bossler 2014). Consistent with these subculture values and norms, hackers' abilities and skills influence their position within their close and larger social networks (Steinmetz 2015). Skilled hackers who are willing to share information with others about successful tactics and tools are central both to the group (Holt et al. 2012) and to the learning experiences of less skilled hackers (Décary-Hétu & Dupont 2012). Novice hackers (known as Script Kiddies) are more peripheral to the group and are encouraged to acquire knowledge about computer technology and hacking techniques through various social networks but mainly through trial and error (Bachmann 2010). To gain status among their peers, hackers may brag about and share their successful operations despite the risk of detection by law enforcement (Jordan & Taylor 1998).

Theoretically Driven Studies

Most of the theoretically driven research that focuses on cyber-dependent offenders draws on either student (Chua & Holt 2016, D'Arcy & Devaraj 2012, Marcum et al. 2014) or organizational employee samples (D'Arcy et al. 2009, Louderback & Antonaccio 2017, Siponen & Vance 2010). As a result, many of these studies focus on relatively low-level acts of cyber-dependent crimes, including guessing passwords to computers, emails, and social media accounts (Bossler & Burruss 2011, Marcum et al. 2014, Morris 2011), misusing computers and computer networks (Louderback & Antonaccio 2017), and violating information security policies (D'Arcy et al. 2009, Hovav & D'Arcy 2012, Hu et al. 2011). The most common criminological traditions that have been applied to explain the etiology of cyber-dependent crime are the General Theory of Crime (Gottfredson & Hirschi 1990), Social Learning (Akers 1973), Social Control [Hirschi (1969) and particularly Sykes & Matza's (1957) techniques of neutralization], and deterrence theories (Gibbs 1975).

The General Theory of Crime suggests that individuals with low self-control are more likely to take advantage of the criminogenic opportunities that they encounter and engage in a wide range of crimes (Gottfredson & Hirschi 1990). Although this theory has earned substantial empirical support among offline offenders (Pratt & Cullen 2000), findings regarding the relationship between individual self-control and involvement in cyber-dependent crimes are mixed. Marcum & associates (2014), for example, reported a significant association between school students' low self-control and their involvement in low forms of hacking. In contrast, Holt & Kilger (2008) found that individuals with high self-control are more likely to hack. Finally, Bossler & Burruss (2011) found that the relationship between self-control and hacking is only significant for individuals with peers who hack. In contrast to these mixed findings, research exploring the relationships between constructs drawn from Social Learning theory and individuals' involvement in cyber-dependent crimes yields more consistent results. The underlying premise behind Social Learning theory states that criminal behavior is learned through a process of imitation and is perpetuated by the influence of peers' positive reinforcement of criminal actions and behavior (Akers 1973). In line with the empirical relationships observed between peer association and individual involvement in offline crimes, several studies indicate that individuals who hack are more likely to have hacking peers (Bossler & Burruss 2011, Skinner & Fream 1997). Hutchings & Clayton (2016) also reported that cyber-dependent criminals who operate websites that illegally offer DDoS attacks for a fee emphasize the influence of others and identified their exposure to these services through gaming and online communities as key factors that influence their involvement in this type of crime.

Several studies have also employed different versions of Social Control theory to explain computer abuse and hacking. Cheng & associates (2013), for example, investigated the effectiveness of Hirschi's (1969) proxies of social bonds, i.e., attachment, belief, involvement, and commitment, in reducing intention to violate information security policies among a sample of organizational employees. These scholars found that attachment to their jobs and to the organization, as well as organizational commitment and norms, significantly decreased employees' intentions to violate organizational information security policies. Other scholars have investigated the relationships between individual uses of techniques of neutralization (Sykes & Matza 1957) and different types of cyber-dependent crimes. Morris (2011), for example, reported that denial of victim is a common neutralizing technique that is used by individuals who participate in low levels of hacking such as password guessing and accessing systems illegally. Taylor (1999) revealed that hackers blame victims for not having the needed technical skills to prevent their victimization. More recently, Chua & Holt (2016) used a cross-national sample of students from the United States, South Africa, and Taiwan to test the relationships between techniques of neutralization and different types of hacking. Their findings revealed that although denial of injury and denial of responsibility were

correlates with simple hacking, appeal to higher loyalties and denial of injury were associated with malware use and creation (however, these findings were consistent for the United States and South Africa samples only). Furthermore, Hutchings & Clayton's (2016) online interviews with 13 operators of websites that offer DDoS attacks as services reveal that the majority of these offenders appeal to higher loyalties to justify their engagement in cyber-dependent crime.

Finally, drawing on the deterrence perspective, empirical attention has been devoted to an exploration of different aspects of sanctions in preventing cyber-dependent crimes. All in all, deterrence theory predicts that when the costs of any behavior outweigh the benefits, an individual should refrain from acting altogether and that punishments perceived to be certain, severe, and swift should be effective in deterring individuals' involvement in crime (Gibbs 1975). Findings regarding the effectiveness of punishment in reducing computer misuse and organizational information security policies are mixed (D'Arcy & Herath 2011). For example, although some research reported that sanction severity reduced intentions to violate information security policies, technology misuse, and computer abuse (Cheng et al. 2013, D'Arcy et al. 2009), other studies found this effect in the United States only (Hovav & D'Arcy 2012), whereas still others did not observe this relationship at all (Hu et al. 2011). Similarly, the effect of sanctions' certainty in reducing intention to misuse information security was found to be significant for specific populations only (D'Arcy et al. 2009, Hovav & D'Arcy 2012). Finally, several studies reported that the effect of sanction celerity is not significant on individuals' violation of information security policies (Hu et al. 2011). Still, Barlow & associates (2013) reported that a clear communication of sanctions is effective in reducing intentions to violate information security policies among employees.

Cyber-Dependent Crime Enablers

Several studies identify the key actors who support the illegitimate activities of cyber-dependent criminals. These enablers include coders or programmers of malicious software, distributors and vendors who trade and sell hacking tools and stolen data, teachers who exchange information regarding cyber-dependent crime techniques and tools, and moderators and administrators of online marketplaces who maintain the criminal infrastructure, vouch for the goods, and enforce social norms in marketplaces (Broadhurst et al. 2014, Dupont et al. 2017, Hutchings & Holt 2015, Leukfeldt et al. 2017). Unfortunately, no extant empirical research focuses solely on enablers' operations. Therefore, what is known about these actors is anecdotal at best. For example, Gordon (2000) reported that malware programmers are not concerned with the effect of their malicious software on their victim. Instead, these enablers' major concern seems to be their reputation and its influence on their potential profit: Several studies reported that malware writers use their handles when advertising the malware they develop and offer for sale on hacker forums and online markets (Chu et al. 2010, Holt & Lampke 2010). Finally, Hutchings & Holt (2015) employed qualitative content analysis of three English- and ten Russian-language forums and reported that vendors on these markets were required to obtain or manufacture their products and then sell them while accepting the verification procedure that their products and services are subject to.

Online Convergence Places

Online offenders and enablers of cyber-dependent crimes meet in either offline or online environments. Leukfeldt & associates (2017), for example, analyzed eighteen Dutch police records that included investigations of cybercriminal groups and reported that cyber-dependent crime offenders who reside in nearby neighborhoods meet in different locations around the city. However, online forums and markets are still considered central for supporting offenders' and enablers'

interactions and recruitment efforts (Hutchings & Holt 2015). The interaction between offenders and enablers over these platforms can be done either publicly or privately (Dupont et al. 2017, Holt et al. 2016). Online forums and market users who employ public communication platforms often create unique public threads that aim at asking a question or advertising a service or a product (Hutchings & Clayton 2016). The posting entity provides a description of the service or product (either needed or provided) and includes details on pricing information, payment, and contact information (Holt & Lampke 2010). These markets offer the hardware, software, and materials needed to initiate all types of cyber-dependent crimes as well as the sensitive data, such as social security numbers, credit card numbers, names, and addresses, that were harvested from victims of cyber-dependent crimes (Yip et al. 2013). Under the private communication model, an interested party can contact the ad owner confidentially, negotiate the details, and, when appropriate, pay for the goods (Holt et al. 2016). Although the interaction between sellers and buyers is mostly confidential, buyers are expected to post their experiences with a seller on the public thread. Similarly to their function in legitimate online markets like Amazon and eBay, the customers' reviews help develop trust and facilitate sellers' reputation (Holt & Lampke 2010, Yip et al. 2013).

Most of the published research that focuses on online convergence places tends to be nontheoretical and descriptive and draws on small samples of market posts that become available to the scholars (Afroz et al. 2013, Holt et al. 2016, Hutchings & Holt 2015). Some of these studies describe the distribution of products and their market pricing (Holz et al. 2009, 2016), whereas one research study presented a crime script analysis for the actions taken by different actors on the markets (Hutchings & Holt 2015). Several studies describe the role of forum administrators in enforcing a broad range of controls, regulations, and reputation management tools over its members, in an effort to discover deviant actors (e.g., Dupont et al. 2017). Other studies consider the social organizations of market networks and the network structures that form in these markets as a function of trust between participants (Dupont et al. 2016, Garg et al. 2015, Yip et al. 2013). Finally, Afroz and associates' (2013) study analyzed the content of five distinctive hacker forums in an effort to distinguish sustainable hacker forums from those that fail. Results from these analyses revealed that sustainable forums tend to employ cheap and easy online community monitoring practices, exhibit a moderate increase in the number of new members, limit members' privileged access, and enforce bans or fines on offending members, and do not witness reduced complexity as the network size increases.

Future Directions for Research

Encouraged by prior research findings regarding the relevance of theoretical criminological concepts in explaining individuals' involvement in cyber-dependent crimes, we believe that scholars should expand their research efforts to include investigations of more types of cyber-dependent crimes as well as more theoretical traditions. For example, more research is needed to understand the role of personality traits, self-control, and cognitive processes in determining an individual's engagement in malware writing and DDoS attacks.

Furthermore, research should draw on the life-course criminology tradition (Sampson & Laub 1993) and explore the criminal trajectories of different cyber-dependent criminals. These studies should be based on research designs that allow the collection of data from both sophisticated and novice hackers and support scholars' efforts to infer causality between key measures. However, beyond the role of personality, we emphasize the role of situational motivation for increasing cyber-dependent crime offenders' potential risk to launch cyber-dependent crimes against large organizations. Briar & Piliavin (1965) suggested that situationally induced stimuli of relatively short

duration can influence individuals' values and behaviors in such a way that leads to a decision to engage in illegal behaviors, independent of their personality traits and commitment to conformity.

Drawing on Briar & Piliavin's (1965) claims, one can identify a wide range of both offline and online situations that could increase online offenders' situational motivation to launch cyber-dependent crimes. For example, the availability of unencrypted data as well as the absence of surveillance on either a computer or computer network could reduce online offenders' risk of detection and punishment and, in turn, increase their probability to launch cyber-dependent crimes (Willison & Siponen 2009). Similarly, political events like wars and military provocations may increase potential online offenders' anger and frustrations and, in turn, increase their situational motivation to launch a cyber-dependent crime against certain targets. Future criminological research should identify situations conducive to cyber-dependent crimes, flag their potential influence on different threat agents, and generate predictions regarding the likelihood of these situations to result in specific types of crimes against individuals and organizations.

More research is also needed about the group of enablers that support the illegitimate operations of online offenders, including about their group ethics (Coleman 2013) and their relationships with both online and offline criminals (Leukfeldt et al. 2017). Concepts discussed by life-course criminologists may be of particular relevance for this group. For example, future research should explore whether cyber-dependent crime offenders who desist from engaging in hacking take upon themselves the role of enablers and move to support cyber-dependent criminals in the shadows as malware writers or administrators on online markets. Other potential explorations could investigate enablers' level of engagement with criminals, whether this engagement is a function of social bonds, and whether they experience desistance from this life-course trajectory as well. Scientific studies should likewise explore whether enablers are amendable by offline and online deterrence-based interventions.

Lastly, future research on online markets should explore how market trends influence cyber-dependent crime risks. For example, would an increase in the availability of malware and attacking tools result in an increase in the volume and frequency of cyber-dependent crimes? Further researching the social relationships, organizational structure, and communication patterns between the different actors that access hacker forums and online environments could also facilitate understanding of online group dynamics and the way they result in different types of online crimes (Dupont et al. 2016). Finally, attention should be given to the effect of disruptive functions (e.g., police crackdowns, price inflation of products) on the interactions between offenders and enablers in online markets as well as on the probability that cyber-dependent crimes are committed. Such investigations could benefit from close collaboration with law enforcement agencies and the deployment of field experiments in these online environments (Afroz et al. 2013, Holt 2017).

TARGETS AND VICTIMS

Given the growing threat of cyber-dependent crimes, it comes as no surprise that Americans today are more worried about having their computers or smartphones hacked than about falling victim to any other type of crime (Riffkin 2014, Yu 2014). In 2016, the Internet Crime Complaint Center, which is the official US government agency that accepts victims' complaints of cybercrime incidents, received more than 27,500 complaints of personal data breaches, more than 3,400 complaints of corporate data breaches, 5,000 reports of malicious malware, and 979 reports of DDoS attacks (FBI 2016). These complaints entailed losses of more than $200 million to the victims. However, victims' unawareness of their own victimization and their unwillingness to report cyber-dependent crimes to law enforcement agencies complicate the task of

estimating the number of victims from these crimes (Bossler & Holt 2013). Several countries have incorporated self-reported victimization items that focus on cyber-dependent crimes in their annual victimization surveys. Findings from the British Crime Survey (BCS 2017), for example, revealed that computer virus (with or without financial loss) and hacking victimization rates were 21 and 12 per 1,000 population, respectively, for the year 2017 in England and Wales. The Eurobarometer survey for 2017 also included data on cyber-dependent victimization (ECPO 2017). Of the four types of cyber-dependent crimes included in the survey, malicious software infection was the most common type (42% of respondents had experienced it in their lifetimes), followed by email/social media account hacking (14%), denial of access to online services (11%), and cyber-extortion (i.e., ransomware, 8%). Importantly, although these victimization surveys indicate that the volume of actual cyber-dependent crime victims is not extremely high, respondents still express high levels of fear of cybercrime (Wall 2013).

At the individual level, a few studies have examined demographic characteristics that are related to increased victimization by cyber-dependent crimes (Bossler & Holt 2009, 2010; Choi 2008; Louderback & Antonaccio 2017; Ngo & Paternoster 2011; Wolfe et al. 2008). These studies found that females are more likely than males to be victimized by hacking or malware infection (Bossler & Holt 2009, 2010; Ngo & Paternoster 2011), whereas there is some evidence that race and ethnicity are not significantly associated with cyber-dependent victimization (Louderback & Antonaccio 2017). Furthermore, evidence on the relationship between age and cyber-dependent victimization is inconsistent, with some studies finding no significant effects (Bossler & Holt 2009, Ngo & Paternoster 2011) and one study finding that older individuals report more hacking attacks based on an adult sample in the Netherlands (Leukfeldt & Yar 2016). Regarding socioeconomic status, van Wilsem (2013) found a negative relationship between education level and hacking victimization using a similar sample of adults from the Netherlands. Finally, people who have higher self-reported cyber-offending (Choi 2008, Wolfe et al. 2008) and peer cyber-offending (Bossler & Holt 2009) are also more likely to experience victimization.

At the organizational level, Rantala (2008) analyzed official data collected by the Bureau of Justice Statistics in 2005 from 7,818 businesses in the United States. The analysis suggests that the telecommunications industry was the most likely industry to be victimized by cyber-dependent crime in 2005, followed by computer system design, chemical and drug manufacturing, and publications and broadcasting. Furthermore, Rantala (2008) found that although the majority of mid- and large-size companies experienced at least one type of cyber-dependent attack, a significant portion of smaller companies (between 44% and 51% of the small companies sampled) reported their victimization from cyber-dependent crimes as well. Lastly, Rantala (2008) found that the majority of cyber-dependent attacks were suspected to be committed by an insider in the particular business, but only 6% of such crimes were reported to law enforcement. A more recent report suggests that because of increasing offender sophistication, malicious code hacks are more difficult to detect and take longer to mitigate, which in turn results in increased costs to the afflicted businesses (Richards et al 2017).

Theoretically Driven Studies

Several criminological theories have been used to explain the relationships between individual characteristics and the likelihood of becoming the victim of cyber-dependent crime. For example, Bossler & Holt (2010) found that low individual self-control was associated with victimization of unauthorized password access and file tampering, yet no significant relationships were reported for malware infection. Similarly, Ngo & Paternoster (2011) reported a nonsignificant association between individuals' self-control and virus infection. Using a rational choice theory framework

and the concept of thoughtfully reflective decision-making (TRDM) (Paternoster & Pogarsky 2009), Louderback & Antonaccio (2017) tested the effects of TRDM on a ten-item scenario-based cyber-deviance index. They found that TRDM reduced cyber-dependent victimization in both student and employee samples, suggesting that cognitive decision-making processes are important in predicting cyber-dependent victimization.

Of all criminological theories, the routine activities perspective (Cohen & Felson 1979) has been applied in most of the victim-based studies of cyber-dependent crime. Typically, the routine activities perspective identifies criminal events as situated in temporal and spatial locations in which motivated offenders, suitable targets, and the absence of capable guardians converge (Cohen & Felson 1979). In line with the extensive empirical support that is reported for this theory when focusing on offline victimization, at both the individual and group levels (Spano & Freilich 2009, Wilcox & Cullen 2018), most prior research that investigated its theoretical claims in cyberspace found moderate support for the theory. Bossler & Holt (2009) found that the absence of social guardianship (e.g., having cyber-deviant peers) increased individuals' chances of data loss from malware infection, whereas physical guardianship (e.g., usage of antivirus software) had no victimization-reduction effect. Similarly, Holt & Bossler (2013) reported that personal guardianship (operationalized as computer skills) reduced individuals' malware victimization, whereas greater involvement in cyber-deviance increased malware victimization. Furthermore, van Wilsem (2013) found that increased computer security measures (i.e., guardianship) reduced hacking victimization, whereas proximity to motivated offenders increased victimization. Several studies also reported that spending long periods of time engaging in online leisure activities (e.g., shopping on e-commerce websites or using social media platforms) increased victimization by adware and spyware (Yucedal 2010), phishing, hacking, and malware (Leukfeldt & Yar 2016, Reyns 2015). Finally, Wang et al. (2015) used Internet traffic data to demonstrate that the visibility, accessibility, and exposure of a target to attacks can increase the probability of cyber-dependent victimization to an insider attack.

In addition to assessing the victimization of cyber-dependent crime at the individual level, several scholars investigated the routine activities premises at the macrolevel as well. Focusing on the time during which large academic institutions are more vulnerable to cyber-dependent crime, Maimon and colleagues (2013) reported that the frequency of computer-focused attacks against a large American university was greater during the organization's business hours (i.e., when there are more suitable targets using their computers) than during any other time of day. These authors also found that increasing the number of the university network's foreign users increased the volume of cyber-dependent crimes from these users' countries of origin. Based on a sample of 132 countries, Kigerl (2012) found that wealthier nations have higher rates of both phishing and spam than do less prosperous countries, which can be due to a greater quantity of suitable targets (i.e., more Internet users) in more affluent nations. Finally, Holt et al. (2016) used data on 30 countries from the open-source Malware Domain List and found that malware infections were more frequent in countries with greater political freedoms and better developed technological infrastructure (i.e., countries with more suitable targets).

Future Directions for Cyber-Dependent Crime Victimization Research

Because most prior research used survey methodologies to collect data from students (Bossler & Holt 2010, Ngo & Paternoster 2011) and employees (Louderback & Antonaccio 2017) in nationally representative samples (Leukfeldt & Yar 2016, van Wilsem 2013), future research should focus attention on other populations such as the elderly, those with limited access to the Internet, and generational cohorts (e.g., millennials versus baby boomers). Data collection should also employ

longitudinal research designs to allow causality modeling between theoretical predictors and cyber-dependent victimization outcomes. Furthermore, deploying experimental field research designs should improve our understanding of cyber-dependent crime victimization as well as the underlying circumstances that increase targets' adoption of self-protective behaviors. Relatedly, the inconsistent operationalization of key theoretical concepts reported by past research may raise questions regarding the validity of these constructs. Future research efforts should seek to generate agreed-upon and standardized metrics of theoretical measures and cyber-dependent crime that have demonstrated validity and reliability (D'Arcy & Herath 2011, Holt & Bossler 2014). This practice would enhance the replication of results and allow meta-analyses to be conducted by including all studies that have used standardized measures of cyber-dependent crime and its predictors.

Researchers should seek to obtain more organizational-level data by collaborating with industry partners to access unique and context-embedded Internet and system-intrusion data. Taking such an approach could support better examination of the way organizational structures and cultures influence the probability of cyber-victimization, both at the organizational and employee levels. Furthermore, scholars should also assess the effectiveness of different cybersecurity awareness campaigns on victimization at the individual and organizational levels. Empirical assessment of the effectiveness of awareness campaigns and training sessions should employ experimental research designs and explore their effect on both short-term and long-term victimization while collecting data from subjects and directly from the Internet (Maimon et al. 2013). Researchers and funding agencies should also work together to fund projects on the incidence, scope, cost, and theoretical predictors of cyber-dependent victimization with nationally representative samples of adults, similar to the National Crime Victimization Survey (Lauritsen & Rezey 2018). Finally, since there is a dearth of research on the effects of the physical environment and one's situational awareness on cyber-dependent victimization, future studies should investigate how physical and technological environments affect victimization.

GUARDIANS

Cohen & Felson's (1979) routine activity theory suggests that the underlying function of a capable guardian is to monitor people and places and to respond rapidly in case a criminal event develops and progresses. In the context of cyber-dependent crimes, the list of relevant guardians includes law enforcement agencies (e.g., the FBI and municipal and local police agencies), governmental nonpolice organizations (e.g., the NSA) that are responsible for managing and monitoring cyberspace, and systems administrators at different ISPs, corporations, and industries, who deploy various technical tools and policies to prevent these crimes from developing and progressing (Grabosky 2016).

Law Enforcement Agencies

One of the major complicating factors in accurately capturing the prevalence of cyber-dependent crimes using official data is law enforcement's lack of familiarity with and knowledge about cybercrime (Broadhurst 2006, Wall 2007). In fact, the findings from a survey of a nonrandom sample of 268 patrol officers in South Carolina and Georgia suggest that local law enforcement officers do not believe it is the role of local law enforcement to investigate cybercrimes (Bossler & Holt 2013). This may be, in part, a function of the training (or, historically, the lack thereof) that local law enforcement personnel receive regarding cybercrime (Fafinski et al. 2010). Findings from this survey further suggest that local police agencies have a limited ability to respond to cyber-dependent crime incidents because of manpower, resource, and budget constraints and that there

is limited interest among officers in various forms of cybercrime and computer training (Bossler & Holt 2013).

Indeed, according to a survey conducted by the Police Executive Research Forum in 2013, almost one-third (29%) of law enforcement agencies surveyed reported that one of the main challenges their agency faced with regard to investigating cybercrime was not having enough staff with sufficient in-house expertise on cybercrime (PERF 2014). Even if there is enough expertise, there may be additional issues with staffing and funding; more than half (54%) of the respondents cited challenges regarding adequate staffing for dedicated cybercrime units, and just under one-third (31%) of respondents referenced a lack a funding for dedicated cybercrime units. These findings may explain why the majority of individuals and businesses who experience cyber-dependent crime victimization do not report their victimization to law enforcement agencies (Rantala 2008).

One approach that PERF (2014) has suggested to address cybercrime encourages the implantation of online community policing programs. However, it is unclear how those online communities should be structured and operated or how effective they would be in preventing cyber-dependent crimes. Furthermore, the effectiveness of police crackdowns (i.e., intensive and focused police efforts that aim to increase the severity and/or certainty of sanctions, along with a public-relations campaign that advertises the operation) (Scott 2003) on hacker forums and dark-net markets in reducing cyber-dependent offenders' involvement in cyber-dependent crimes is still unknown. Another approach calls for increasing formal deterrence efforts through the establishment of international legislation and cross-national collaborations between law enforcement agencies. Focusing on the potential deterring effect of the 2001 Convention on Cybercrime (COC), the first international legislation against criminal behavior in cyberspace, Hui & associates (2017) estimated the impact of this convention on the volume of DDoS attacks against enforcing countries. Analyzing data comprising a sample of real DDoS attacks recorded in 106 countries in 177 days between 2004 and 2008, these scholars reported that enforcing the COC decreased DDoS attacks by at least 11.8%. Furthermore, they found evidence of network and displacement effects in COC enforcement: Nonenforcing countries reported higher levels of DDoS attacks after the implementation of the COC legislation compared to enforcing countries.

System Administrators and Technical Tools

To facilitate safe and secure Internet infrastructures, many corporations and individuals use designated protocols, technical tools, and security policies that aim to configure the online environment in such a way that reduces the probability of cyber-dependent crimes from occurring and progressing. For example, antivirus software, firewalls, and intrusion detection/prevention systems are commonly used by large organizations to prevent the progression of cyber-dependent crimes (McHugh 2000). These tools are designed to detect cyber-dependent crimes and security violations, prevent them from developing, and provide useful information to system administrators who are responsible for recovering from cyber-dependent crimes. These and other approaches to prevent cyber-dependent crimes coincide with the list of crime prevention strategies that are recommended by the situational crime prevention (SCP) perspective (Cornish & Clarke 2003) to prevent the occurrence of offline crimes.

In brief, the underlying premise of the SCP perspective is that criminals are rational creatures who weigh the costs and benefits of their behaviors, so successful crime prevention efforts must involve the design and manipulation of human environments to make offenders' decisions to get involved in crime less attractive (Clarke 1995). The growing volume of cyber-dependent crime incidents during the past fifteen years has led criminologists and information scientists around

the world to review the applicability of the SCP perspective in the context of different types of online crime. Coles-Kemp & Theoharidou (2010) focused on insider threats to information security, Morris et al.'s (2004) work focused on malicious software, and Brookson & colleagues (2007) applied SCP in the context of hacking. However, despite the growing number of individuals and organizations that implement security tools and policies in their computing environments, empirical investigations that assess the effectiveness of these strategies in preventing and mitigating malicious cyber-dependent operations are still relatively scarce (Denning & Baugh 2000, Harknett et al. 2010). In fact, only two recent studies (Lévesque et al. 2013, 2016) employed clinical trials to assess the effectiveness of antivirus products in detecting and preventing malware infections among computer users.

Antivirus software is designed to keep computer devices clean from malicious software (malware) such as viruses, worms, and trojans and is commonly deployed on computers and smartphones as the last line of defense against cyber-dependent crimes (Al-Ghaith 2016). In Lévesque et al. (2013), the authors recruited 50 participants from the Université de Montréal campus, provided them with new laptops, and monitored these participants' real-world computer usage using various diagnostic tools over a period of four months. The authors reported that almost one out of two newly installed laptops would have been infected with malware within four months if the computers had no antivirus software installed. Furthermore, these scholars found that 20% of the study computers were infected by some form of malicious software that was not detected by the antivirus software installed on the machine. In another study, Lévesque and colleagues (2016) monitored close to 27 million Windows 10 systems for a period of four months to test the probability of these computers being infected with malware. The scholars were able to differentiate between systems that were protected by a third-party antivirus product (the treatment group) and systems that were protected by Microsoft Windows Defender, Microsoft's default antivirus software (the control group). The authors found that 1.22% of the computer systems in the treatment group were infected by malware during the experimental period. In contrast, 14.95% of the computer systems in the control group could have been infected by malware if no antivirus product were protecting the system. A comparison of the effectiveness of the 10 most prevalent antivirus products (more than 90% of the systems were protected by third-party software) revealed that the effectiveness of these products in detecting malicious software ranged from 90% to 98%.

Theoretically Driven Research

Several studies have tested how two different aspects of guardianship, warning and surveillance, influence the progression of cyber-dependent crimes (Maimon et al. 2014, Testa et al. 2017, Wilson et al. 2015). These studies adopted Gibbs's (1975) conceptualization of restrictive deterrence to guide their empirical investigations. Maimon and colleagues (2014), for example, tested the effect of a warning banner in an attacked computer system on the progression, frequency, and duration of system-trespassing events. To answer these research questions, the authors deployed a large set of target computers built for the sole purpose of being attacked (i.e., honeypots) on the Internet infrastructure of a large American university and conducted two randomized experiments in which the target computers were set either to display or not to display a warning banner once hackers had successfully infiltrated the systems. Findings from these two experiments revealed that a warning banner did not lead to the immediate termination or a reduction in the frequency of trespassing incidents. Nevertheless, the average duration of system-trespassing incidents recorded on the target computers with a warning banner was significantly shorter than the average duration of those incidents recorded on target computers with no warning banners (the differences were observed for both the first system-trespassing incidents recorded on each of the target computers

and the overall set of incidents recorded during the experimental period). Furthermore, these authors reported that the effect of a warning message on the duration of repeated trespassing incidents was attenuated in computers with a large bandwidth capacity. Stockman et al. (2015) replicated Maimon & colleagues' (2014) research design and offered support for these findings.

Testa and colleagues (2017) further explored the effect of a warning banner in mitigating hackers' levels of activity (i.e., roaming the attacked system and manipulating file permission) in an attacked computer system while taking into account the level of administrative privileges imposed by the system trespasser on the attacked computer. Using the data collected by Maimon & colleagues (2014) in their second experiment, Testa & associates (2017) reported that the presence of a warning banner on an attacked computer system had no statistically significant effect on the probability of either navigation or file permission change commands being entered on the system. However, when testing the effect of the warning banner on computers attacked by system trespassers with nonadministrative privileges, these authors reported that a warning banner substantially reduced the use of both navigation and change file permission commands compared to the no-warning computers.

Focusing on the monitoring aspect of online guardianship, Wilson & associates (2015) sought to determine (*a*) whether a surveillance banner displayed to system trespassers upon entry to a computer system reduced the probability of computer commands being entered into the compromised system during the first system-trespassing incident, (*b*) how effective a surveillance banner was in reducing the volume and probability of repeated system-trespassing incidents on a target computer, and (*c*) whether the effect of a surveillance banner on an intruder's decision to enter commands in the system decayed during subsequent system-trespassing incidents. These scholars collected data using target computers deployed on the Internet infrastructure of a large American university for a period of seven months and followed a 2×2 (surveillance banner versus no surveillance banner $\times$ surveillance program versus no surveillance program) experimental research design. They found that the presence of a surveillance banner in the attacked computer systems reduced the probability of commands being typed in the system during longer first system-trespassing incidents. Further, they reported that the probability of commands being typed during subsequent system-trespassing incidents (on the same target computer) was conditioned by the presence of a surveillance banner and by whether commands had been entered during previous trespassing incidents. However, the surveillance banner was found to be ineffective in reducing the volume and probability of repeated system-trespassing incidents on a target computer.

In addition to tracking guardians' efforts to influence cyber-dependent criminal operations using deterrence-based strategies, extensive research has investigated ways in which guardians could influence targets' decision to implement self-protective behaviors and comply with organizational cybersecurity policies, using both rewards and punishments (Herath & Rao 2009, Johnston & Warkentin 2010, Siponen et al. 2010). This line of research draws on protection motivation theory (PMT) (Rogers 1975), which suggests that individuals are more likely to protect themselves from potential risks after receiving fear-arousing recommendations. According to the theory, two processes and outcomes must occur for a person to engage in an adaptive response. First, in the threat-appraisal process, the threat and generated fear that inspire protection motivation must be weighted more heavily than the maladaptive rewards earned by not engaging in protection motivation. Second, in the coping-appraisal process, a person's response efficacy and self-efficacy must outweigh the response costs for engaging in the protection motivation (Rogers 1975).

Most of the empirical research that employed PMT has analyzed data collected from samples of organizational employees. Herath & Rao (2009) found that employees made inaccurate predictions about the probability of actually experiencing a security breach, which in turn results in noncompliance with security policies. In contrast, employees' accurate assessment of their

organizational vulnerability to information security threats was found to have a significant effect on their intentions to comply with security policies (Siponen et al. 2010). Furthermore, Workman and colleagues (2008) reported that employees' subjective assessment of risk severity to a breach of their confidential information and their perceived vulnerability to cyber-dependent crime were negatively associated with self-reported failure to apply security solutions.

Johnston & Warkentin (2010) tested the effects of fear appeals and the enactment of computer security behaviors to mitigate threats among a sample of students, faculty, and employees of a large university. Their main findings suggest that there is an overall positive effect of fear appeal on use of computer security behaviors, but this effect differs in magnitude across users and based on the individual's level of self-efficacy, threat severity, social influence, and response efficacy. Boss and associates (2015) confirmed this finding by employing both survey-based and experimental research designs. These findings are also consistent with Siponen & associates' (2010) report that persuasive messages regarding the need for security compliance should be communicated clearly and in a visible manner, for employees to comply with security policies. Finally, sanctions for noncompliance with security policies were found to be positively associated with employees' actual compliance with organizational security policy (Siponen et al. 2010). Still, no prior research has investigated whether employees' compliance with organizational security policies reduces the organization's risk of cyber-dependent crime victimization.

Future Directions for Research

Rigorous evidence regarding the effectiveness of guardians in preventing and mitigating cyber-dependent crimes is still relatively limited. Future research should further investigate the ways in which the presence (either online or offline) and function of guardians prevent and disrupt the progression of cyber-dependent crimes. Such research should explore the influence of both social and technical guardians on offender and target behaviors in cyberspace. In that sense, we believe that guardian operations should employ the data available on online markets and hacker forums to generate predictions regarding the occurrence, timing, and progression of cyber-dependent crimes. As elsewhere, one of the major hurdles in this area could be the absence of universally accepted measurement metrics, which would provide guardians and scholars with practical techniques for assessing the effectiveness of policing efforts, security policies, and tools in preventing cyber-dependent crimes (Torres et al. 2006). Indeed, the most common approach to the implementation of preventive practices in online environments draws on guardians' personal experiences in the field as well as their personal worldviews when making security-related decisions that may influence offenders and targets (Siponen & Willison 2009). Such an approach does not require rigorous empirical evaluations of security tools and policies to support the decision-making by these professionals. However, Blakely (2002) suggested that this approach has failed to prevent individuals and organizations from becoming the targets and victims of cyber-dependent crimes. Therefore, Blakely proposed the adoption of an approach that monetizes guardianship efforts and called for quantifying the effectiveness of security tools and policies in achieving their stated goals.

Future research should seek to evaluate the most effective way to successfully implement security controls and protocols, policies, and tools in online environments as well as to assess the effectiveness of these approaches in preventing and mitigating the consequences of cyber-dependent crimes. Such evaluations should include the development of security metrics that are clear, objective, repeatable, and simple (Atzeni & Lioy 2006). In addition, we believe that future criminological research should further explore how different configurations of online environments shape both online offender and target involvement in cyber-dependent crimes

(Lessig 2009). Encouraged by findings reported in the criminological literature indicating that environmental design could reduce the volume of robbery (Jeffrey et al. 1987), vandalism (Sloan-Howitt & Kelling 1990), teenagers' joy riding (Bell & Burke 1992), and shoplifting (Farrington & Burrows 1993) incidents, we believe that guardians' familiarity with computer and online configurations that result in lower rates of and less damage from cyber-dependent crimes could guide the design of safer online environments.

DISCUSSION

Our major objective in this review is to expose readers to the current state of knowledge in criminologically driven cyber-dependent crimes research. After reviewing the interdisciplinary scholarship available for each of the key actors who operate within the cyber-dependent crime ecosystem, we highlighted areas in which we believe future research is still needed. However, we suspect that criminologists' familiarity with the cybercrime ecosystem or their acknowledgment of the full extent of the societal effects of cyber-dependent crime (Diamond & Bachmann 2015) will not suffice for bringing cybercrime scholarship to the forefront of the criminological field. We submit that for the criminological community to accept the centrality of cyber-dependent crime research to our field, contemporary cyber-criminologists, as well as information scientists and cybersecurity experts who employ criminological reasoning in their research, should think about ways in which their work may advance current criminological theoretical discourses. Ideally, these efforts will offer unique research designs that allow the implementation of unique methodologies and will be relevant both to public policy discussion and to the construction of new technical tools.

Theory

As indicated in this interdisciplinary review, several criminological theories provide important frameworks that guide empirical investigations of different junctures within the cyber-dependent crime ecosystem. However, most of the prior theoretically driven research merely sought to investigate the effectiveness of criminological concepts in explaining cyber-dependent crime offending (Bossler & Burruss 2011, Marcum et al. 2014) or victimization (Bossler & Holt 2009, Holt & Bossler 2013). Unfortunately, those studies do not really push the theoretical envelope beyond our current understanding of their respective theoretical frameworks and do not expose the criminological community to new and exciting theoretical insights in the context of the online environment. Cybercrime scholars should reflect upon different aspects of existing criminological explanations of crime that could be better understood in the context of the online environment. One potential example of a criminological theory that could benefit from cyber-dependent crime research is the criminal event perspective (Meier et al. 2001).

The criminal event perspective focuses on the microsocial level of illegal behaviors and goes beyond offenders' motivation to include insights regarding the interactions among criminal event participants, the unfolding of criminal events, and the settings in which these events occur, as all three are parts of the etiology of crime (Short 1998). This approach suggests that a comprehensive explanation of crime should incorporate knowledge regarding the way offenders and victims present themselves and interact and that the settings in which these interactions occur shape the interactive process between actors (Meier et al. 2001). However, although advocates of the criminal event perspective believe this approach is relevant for all types of predatory crimes, prior studies employing this perspective have only focused on the interactional processes leading to violent offenses (Deibert & Miethe 2003, Fagan & Wilkinson 1998, Luckenbill 1977). Still,

these studies do not draw on a cohesive theoretical model that allows the development of clear research hypotheses regarding the interactions between offenders and victims, or those regarding the progression of a criminal event. Since cyber-dependent crimes occur in online environments that support the collection of data from the actual interaction (both network and human) between offenders, victims, and guardians, cybercrime scholars could take advantage of this unique research setting and theorize about the progression of criminal events. Conceptualization is key to understanding and generating predictions regarding the progression of online crimes but may also be of relevance in the context of offline crimes.

Methodologies and Research Designs

Alongside the limited contribution to contemporary theoretical traditions, most of the research reported in this work exhibits serious data limitations that may call into question the conclusions made by the authors [both Bossler (2017) and Diamond & Bachmann (2015) acknowledge this problem in their assessments of cybercrime scholarship]. To begin, most of the research around cyber-dependent crime draws on convenient samples of college students (Bossler & Holt 2010, Chua & Holt 2016) or organizational employees (Cheng et al. 2013). Similarly, the extensive research on online convergence sites draws on small samples of publicly available posts from online markets that were accessible to scholars (Holt 2017). This fact complicates researchers' abilities to draw statistical conclusions about the representativeness of the sample. As such, findings based on these analyses may not represent the population from which they are drawn. Future research should seek to apply research designs that allow the collection of data across the life course using longitudinal data and cross-national comparisons of the frequency and correlates of cybercrime offending and victimization. Future studies should also employ more quasi-experimental and experimental research designs to obtain more valid and reliable empirical findings on the actual incidence and predictors of cyber-dependent crimes. The implementation of such research designs would allow a better understanding of the causal mechanisms underlying cyber-offending and victimization by reducing or eliminating the effects of confounding factors in these empirical relationships. By using an experimental approach with innovative technology such as real-time user and system-intrusion tracking on smartphones (Jeong et al. 2016, Park et al. 2014), researchers will be better able to collect, manage, and analyze empirical data on cyber-dependent crimes.

Importantly, using survey measurement approaches for constructing cyber-dependent crime measures (e.g., phishing, hacking, DDoS, ransomware) may result in the underestimation of cyber-dependent crime reports. Because knowledge about cybercrime is limited among the general public, survey participants may not know if they have been victimized by a specific type of cybercrime. Using this measurement approach may empirically measure computer skills, knowledge, and expertise, as individuals with higher proficiency in these areas would be more likely to correctly identify the type(s) and frequency of cybercrimes that they have encountered. Although some research has sought to rectify this methodological issue by using actual system-intrusion data (Maimon et al. 2013) and honeypot decoy computers (Bringer et al. 2012, Maimon et al. 2014), as well as by using graphical scenario-based measures of various types of cybercrime (Louderback & Antonaccio 2017), future research should further address this issue and collect records on cyber-dependent crimes directly from the devices and networks of individuals who were engaged in these crimes.

Relatedly, scholars across disciplines should collectively develop universal measures of key concepts in cyberspace to guide future empirical analyses, to ensure consistency, and to facilitate more interdisciplinary research collaborations. This coordinated research effort would enhance the accurate and rigorous study of behaviors and processes in the cybersecurity ecosystem, which would

maximize the scholarly consensus about key concepts and their operationalization. Furthermore, by obtaining valid and reliable data on key concepts at the individual level, researchers could move toward aggregating these microlevel measures to the macrolevel (e.g., in neighborhoods), an established method in ecological research on property and violent crime (Sampson 2012). These macrolevel cyber-dependent crime measures could then be mapped using geographic information systems and geospatial analysis methods (Bunting et al. 2018, Graif & Sampson 2009) to examine local and global trends as well as the clustering of cyber-dependent crimes within and across neighborhoods, states, and nations.

Policy Implications

Because the Internet is an environment that can be regulated and configured based on desires and needs (Lessig 2009), governmental agencies, private corporations, and individuals around the globe employ a wide range of technical tools and security policies in their efforts to reduce their probability of becoming victims of cyber-dependent crimes. Nevertheless, the effectiveness of these strategies in preventing and mitigating the occurrence of hacking, DDoS attacks, and distribution of malware is still relatively unknown. For example, one important policy often incorporated into contemporary computing environments is the implementation of surveillance means in users' computer systems (Eivazi 2011). The application of surveillance and monitoring in computing environments is intended to increase deterrence and social control by increasing the probability of rapid detection of an undesired use of computer systems, whether by legitimate (D'Arcy & Herath 2011) or illegitimate users (Hsiao et al. 2014). However, despite the growing number of individuals and organizations that implement these tools and policies in their computing environments, the effectiveness of these strategies in preventing and mitigating the occurrence of malicious cyber-activities is still relatively unclear (Denning & Baugh 2000). Criminological research could generate insights that may pave the way for the implantation of safer cyber-environments that prevent these crimes from occurring and mitigate their consequences to victims. By communicating policy-relevant issues to public policymakers as well as information security personnel in different types of organizations, cyber-criminologists could investigate research topics that will have both theoretical and policy relevance. In this sense, we believe that criminological attention to cyber-dependent crimes can help guide the design of computer systems, education programs (Papanikolaou et al. 2013), and pre-employment testing to create security tools that account for the human factor in computer-dependent crimes.

CONCLUSION

The expansion of cyber-dependent crimes in the United States and around the globe has increased the need for extensive research in this area. However, the complex nature of this new type of crime necessitates interdisciplinary research efforts by criminologists, information scientists, computer scientists, and cybersecurity experts. This may result in marginalization of this research area by the mainstream criminological community. To prevent this from happening, criminologists who study this type of crime should spark interest in cybercrime research among both young and established scholars in our field. The current body of published work on cyber-dependent crime provides an excellent foundation for continued research in this area. However, to bring this line of research into the forefront of criminology, scholars engaged in it should make sure their studies advance current criminological traditions, involve the collection of unique valid and reliable data, and possess relevance to public policy discussion.

DISCLOSURE STATEMENT

The authors are not aware of any affiliations, memberships, funding, or financial holdings that might be perceived as affecting the objectivity of this review.

LITERATURE CITED

Afroz S, Garg V, McCoy D, Greenstadt R. 2013. Honor among thieves: a common's analysis of cybercrime economies. *eCrime Res. Summit* 2013:1–11

Akers RL. 1973. *Deviant Behavior: A Social Learning Approach*. Belmont, CA: Wadsworth Publ.

Al-Ghaith W. 2016. Extending protection motivation theory to understand security determinants of anti-virus software usage on mobile devices. *Int. J. Comput.* 10:125–38

Atzeni A, Lioy A. 2006. Why to adopt a security metric? A brief survey. In *Quality of Protection. Advances in Information Security*, Vol. 23, ed. D Gollmann, F Massacci, A Yautsiukhin, pp. 1–12. Boston: Springer

Bachmann M. 2010. The risk propensity and rationality of computer hackers. *Int. J. Cyber Criminol.* 4:643–56

Barlow JB, Warkentin M, Ormond D, Dennis AR. 2013. Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Comput. Secur.* 39:145–59

Bell J, Burke B. 1992. *Cruising Cooper Street Situational Crime Prevention*: *Successful Case Studies*. Guilderland, NY: Harrow and Heston. 2nd ed.

Blakley B. 2002. The measure of information security is dollars. In *Proceedings of the First Annual Workshop on the Economics of Information Security*. Berkeley, CA: Univ. Calif. Press

Boss SR, Galletta DF, Lowry PB, Moody GD, Polak P. 2015. What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Q.* 39:837–64

Bossler AM. 2017. Need for debate on the implications of honeypot data for restrictive deterrence policies in cyberspace. *Criminol. Public Policy* 16:681–88

Bossler AM, Burruss GW. 2011. The general theory of crime and computer hacking: low self-control hackers. In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, ed. TJ Holt, BH Schell, pp. 38–67. Hershey, PA: IGI Glob.

Bossler AM, Holt TJ. 2009. On-line activities, guardianship, and malware infection: an examination of routine activities theory. *Int. J. Cyber Criminol.* 3:400–20

Bossler AM, Holt TJ. 2010. The effect of self-control on victimization in the cyberworld. *J. Crim. Justice* 38:227–36

Bossler AM, Holt TJ. 2013. Assessing officer perceptions and support for online community policing. *Secur. J.* 26:349–66

Briar S, Piliavin I. 1965. Delinquency, situational inducements, and commitment to conformity. *Soc. Probl.* 13:35–45

Bringer ML, Chelmecki CA, Fujinoki H. 2012. A survey: recent advances and future trends in honeypot research. *Int. J. Comput. Network Inf. Secur.* 4:63–75

Br. Crime Surv. (BCS). 2017. Table E1: Fraud and computer misuse by loss (of money or property) - number and rate of incidents and number and percentage of victims, year ending September 2017 CSEW (Official Statistics).

Broadhurst R. 2006. Developments in the global law enforcement of cyber-crime. *Polic. Int. J. Police Strateg. Manag.* 29:408–33

Broadhurst R, Grabosky P, Alazab M, Bouhours B, Chon S. 2014. An analysis of the nature of groups engaged in cyber crime. *Int. J. Cyber Criminol.* 8:1–20

Brookson C, Farrell G, Mailley J, Whitehead S, Zumerle D. 2007. ICT product proofing against crime. *ETSI White Paper* 5:1–33

Bunting RJ, Chang OY, Cowen C, Hankins R, Langston S, et al. 2018. Spatial patterns of larceny and aggravated assault in Miami-Dade County, 2007–2015. *Prof. Geogr.* 70:34–46

Chen H, Chiang RH, Storey VC. 2012. Business intelligence and analytics: from big data to big impact. *MIS Q.* 36:1165–88

Cheng L, Li Y, Li W, Holm E, Zhai Q. 2013. Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. *Comput. Secur.* 39:447–59

Chu B, Holt TJ, Ahn GJ. 2010. *Examining the Creation, Distribution, and Function of Malware On-line*. Washington, DC: Natl. Inst. Justice

Choi KS. 2008. Computer crime victimization and integrated theory: an empirical assessment. *Int. J. Cyber Criminol.* 2:308–33

Chua YT, Holt TJ. 2016. A cross-national examination of the techniques of neutralization to account for hacking behaviors. *Vict. Offenders* 11:534–55

Clarke RV. 1995. Situational crime prevention. *Crime Justice* 1:91–150

Cohen LE, Felson M. 1979. Social change and crime rate trends: a routine activity approach. *Am. Sociol. Rev.* 44:588–608

Coles-Kemp L, Theoharidou M. 2010. Insider threat and information security management. In *Insider Threats in Cyber Security*, ed. J Hunker, D Gollman, pp. 45–71. Boston: Springer

Coleman EG. 2013. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton, NJ: Princeton Univ. Press

Cornish DB, Clarke RV. 2003. Opportunities, precipitators and criminal decisions: a reply to Wortley's critique of situational crime prevention. *Crime Prev. Stud.* 16:41–96

D'Arcy J, Devaraj S. 2012. Employee misuse of information technology resources: testing a contemporary deterrence model. *Decis. Sci.* 43:1091–124

D'Arcy J, Herath T. 2011. A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *Eur. J. Inf. Syst.* 20:643–58

D'Arcy J, Hovav A, Galletta D. 2009. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Inf. Syst. Res.* 20:79–98

Décary-Hétu D, Dupont B. 2012. The social network of hackers. *Glob. Crime* 13:160–75

Deibert GR, Miethe TD. 2003. Character contests and dispute-related offenses. *Deviant Behav.* 24:245–67

Denning D, Baugh W. 2000. Hiding crimes in cyberspace. In *Cybercrime: Law Enforcement' Security and Surveillance in the Information Age*, ed. D Thomas, D Loader, pp. 105–32. London: Routledge

Dey D, Lahiri A, Zhang G. 2012. Hacker behavior, network effects, and the security software market. *J. Manag. Inf. Syst.* 29:77–108

Diamond B, Bachmann M. 2015. Out of the beta phase: obstacles, challenges, and promising paths in the study of cyber criminology. *Int. J. Cyber Criminol.* 9:24–34

Dupont B, Côté AM, Boutin JI, Fernandez J. 2017. Darkode: recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world." *Am. Behav. Sci.* 61:1219–43

Dupont B, Côté AM, Savine C, Décary-Hétu D. 2016. The ecology of trust among hackers. *Glob. Crime* 17:129–51

Duncan OD. 1961. From social system to ecosystem. *Sociol. Inq.* 31:140–49

Dunlap RE, Catton WR Jr. 1979. Environmental sociology. *Annu. Rev. Sociol.* 5:243–73

Eivazi K. 2011. Computer use monitoring and privacy at work. *Comput. Law Sec. Rev.* 27:516–23

Eur. Comm. Public Opin. (ECPO). 2017. *Eurobarometer: Europeans' Attitudes Towards Cyber Security*. Brussels, Belg.: Eur. Union

Fafinski S, Dutton WH, Margetts H. 2010. *Mapping and measuring cybercrime*. Oxf. Int. Inst. Work. Pap. No. 18

Fagan J, Wilkinson DL. 1998. Social contexts and functions of adolescent violence. In *Violence in American Schools: A New Perspective*, ed. DS Elliott, BA Hamburg, KR Williams, pp. 55–93. New York: Cambridge Univ. Press

Farrington DP, Burrows JN. 1993. Did shoplifting really decrease? *Br. J. Criminol.* 33:57–69

Fed. Bur. Investig. (FBI). 2017. *2016 IC3 Annual Report*. Washington, DC: Bur. Justice Stat. **http://www.ic3.gov/media/annualreport/2016_IC3Report.pdf**

Furnell S. 2002. *Cybercrime: Vandalizing the Information Society*. Boston: Addison-Wesley

Furnell S, Emm D, Papadaki M. 2015. The challenge of measuring cyber-dependent crimes. *Comput. Fraud Secur.* 2015:5–12

Garg V, Afroz S, Overdorf R, Greenstadt R. 2015. Computer-supported cooperative crime. *Int. Conf. Financ. Cryptogr. Data Secur.* 2015:32–43

Gibbs J. 1975. *Crime, Punishment, and Deterrence*. New York: Elsevier
Glenny M. 2011. *Darkmarket: Cyberthieves, Cybercops and You*. New York: Random House
Gordon S. 2000. *Virus writers: the end of the innocence*? Paper presented at the 10th Annual Virus Bulletin Conference (VB2000), Orlando, FL, Sept. 28–29
Gottfredson MR, Hirschi T. 1990. *A General Theory of Crime*. Stanford: Stanford Univ. Press
Grabosky P. 2016. The evolution of cybercrime, 2006–2016. In *Cybercrime Through an Interdisciplinary Lens*, ed. TJ Holt, pp. 15–37. New York: Routledge
Graif C, Sampson RJ. 2009. Spatial heterogeneity in the effects of immigration and diversity on neighborhood homicide rates. *Homicide Stud*. 13:242–60
Harknett RJ, Callaghan JP, Kauffman R. 2010. Leaving deterrence behind: war-fighting and national cybersecurity. *J. Homel. Secur. Emerg. Manag.* 7:22
Hartley RD. 2015. Ethical hacking pedagogy: an analysis and overview of teaching students to hack. *J. Int. Technol. Inf. Manag.* 24:95–104
Herath T, Rao HR. 2009. Protection motivation and deterrence: a framework for security policy compliance in organisations. *Eur. J. Inf. Syst.* 18:106–25
Hirschi T. 1969. *Causes of Delinquency*. Piscataway, NJ: Transaction Publ.
Holt TJ. 2007. Subcultural evolution? Examining the influence of on- and off-line experiences on deviant subcultures. *Deviant Behav*. 28:171–98
Holt TJ. 2017. On the value of honeypots to produce policy recommendations. *Criminol. Public Policy* 16:739–47
Holt TJ, Bossler AM. 2013. Examining the relationship between routine activities and malware infection indicators. *J. Contemp. Crim. Justice* 29:420–36
Holt TJ, Bossler AM. 2014. An assessment of the current state of cybercrime scholarship. *Deviant Behav*. 35:20–40
Holt TJ, Bossler AM. 2016. *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. New York: Routledge
Holt TJ, Bossler AM, May DC. 2012. Low self-control deviant peer associations and juvenile cyberdeviance. *Am. J. Crim. Justice* 37:378–95
Holt TJ, Burruss GW, Bossler AM. 2016. Assessing the macro-level correlates of malware infections using a routine activities framework. *Int. J. Offender Ther. Comp. Criminol.* 62:1720–41
Holt TJ, Kilger M. 2008. Techcrafters and makecrafters: a comparison of two populations of hackers. In *IEEE Information Security Threats Data Collection and Sharing Workshop*, pp. 67–78. New York: IEEE
Holt TJ, Lampke E. 2010. Exploring stolen data markets online: products and market forces. *Crim. Justice Stud.* 23:33–50
Holz T, Engelberth M, Freiling F. 2009. Learning more about the underground economy: A case-study of keyloggers and dropzones. *Eur. Symp. Res. Comput. Secur.* 2009:1–18
Hovav A, D'Arcy J. 2012. Applying an extended model of deterrence across cultures: an investigation of information systems misuse in the US and South Korea. *Inf. Manag.* 49:99–110
Hsiao DK, Kerr DS, Madnick SE. 2014. *Computer Security*. Cambridge, MA: Academic Press
Hu Q, Xu Z, Dinev T, Ling H. 2011. Does deterrence work in reducing information security policy abuse by employees? *Commun. ACM* 54:54–60
Hughes LA, DeLone GJ. 2007. Viruses, worms, and trojan horses: serious crimes, nuisance, or both? *Soc. Sci. Comput. Rev.* 25:78–98
Hui KL, Kim SH, Wang QH. 2017. Cybercrime deterrence and international legislation: evidence from distributed denial of service attacks. *MIS Q.* 41:497–523
Hutchings A, Clayton R. 2016. Exploring the provision of online booter services. *Deviant Behav*. 37:1163–78
Hutchings A, Holt TJ. 2015. A crime script analysis of the online stolen data market. *Br. J. Criminol.* 55:596–614
Jeffrey CR, Hunter RD, Griswold J. 1987. Crime prevention and computer analysis of convenience store robberies in Tallahassee. *Fla. Police J.* 34:65–69
Jeong ES, Kim IS, Lee DH. 2016. SafeGuard: a behavior based real-time malware detection scheme for mobile multimedia applications in android platform. *Multimed. Tools Appl.* 76:18153–73

Johnston AC, Warkentin M. 2010. Fear appeals and information security behaviors: an empirical study. *MIS Q*. 34:549–66
Jordan T, Taylor P. 1998. A sociology of hackers. *Sociol. Rev.* 46:757–80
Karami M, Park Y, McCoy D. 2016. Stress testing the booters: understanding and undermining the business of DDoS services. In *Proceedings of the 25th International Conference on World Wide Web*, pp. 1033–43. Geneva, Switz.: Int. World Wide Web Conf. Steer. Comm.
Kigerl A. 2012. Routine activity theory and the determinants of high cybercrime countries. *Soc. Sci. Comput. Rev.* 30:470–86
Kraemer-Mbula E, Tang P, Rush H. 2013. The cybercrime ecosystem: online innovation in the shadows? *Technol. Forecast. Soc. Change* 80:541–55
Kremling J, Parker AM. 2017. *Cyberspace, Cybersecurity, and Cybercrime*. Thousand Oaks, CA: SAGE
Lauritsen JL, Rezey ML. 2018. Victimization trends and correlates: Macro- and microinfluences and new directions for research. *Annu. Rev. Criminol.* 1:103–21
Lessig L. 2009. *Code: And Other Laws of Cyberspace, Version 2.0*. New York: Basic Books
Leukfeldt R, Kleemans E, Stol W. 2017. Origin, growth and criminal capabilities of cybercriminal networks. An international empirical analysis. *Crime Law Soc. Change* 67:39–53
Leukfeldt ER, Yar M. 2016. Applying routine activity theory to cybercrime: a theoretical and empirical analysis. *Deviant Behav*. 37:263–80
Lévesque LF, Nsiempba J, Fernandez JM, Chiasson S, Somayaji A. 2013. A clinical study of risk factors related to malware infections. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, pp. 97–108. New York: ACM
Lévesque FL, Fernandez JM, Batchelder D, Young G. 2016. Are they real? Real-life comparative tests of antivirus products. In *Virus Bulletin Conference*, pp. 1–11. Abingdon, UK: Virus Bull.
Lewis JA. 2018. *Economic impact of cybercrime: at $600 billion and counting—no slowing down*. CSIS Rep., Cent. Strateg. Int. Stud., Washington, DC. **https://www.csis.org/analysis/economic-impact-cybercrime**
Louderback ER, Antonaccio O. 2017. Exploring cognitive decision-making processes, computer-focused cyber deviance involvement and victimization: the role of thoughtfully reflective decision-making. *J. Res. Crime Delinquency* 54:639–79
Luckenbill DF. 1977. Criminal homicide as a situated transaction. *Soc. Probl.* 25:176–86
Luo X, Liao Q. 2009. Ransomware: a new cyber hijacking threat to enterprises. In *Handbook of Research on Information Security and Assurance*, ed. JND Gupta, S Sharma, pp. 1–6. Hershey, PA: IGI Glob.
Macdonald M, Frank R. 2017. The network structure of malware development, deployment and distribution. *Glob. Crime* 18:49–69
Maimon D, Alper M, Sobesto B, Cukier M. 2014. Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology* 52:33–59
Maimon D, Kamerdze A, Cukier M, Sobesto B. 2013. Daily trends and origin of computer-focused crimes against a large university computer network. *Br. J. Criminol.* 53:319–43
Marcum CD, Higgins GE, Ricketts ML, Wolfe SE. 2014. Hacking in high school: cybercrime perpetration by juveniles. *Deviant Behav*. 35:581–91
McGuire M. 2012. *Organised Crime in the Digital Age*. London: John Grieve Cent. Polic. Secur.
McGuire M, Dowling S. 2013. *Cyber crime: a review of the evidence. Summary of key findings and implications*. Home Off. Res. Rep., Home Off., London
McHugh J. 2000. Testing intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection system evaluations as performed by Lincoln laboratory. *ACM Trans. Inf. Syst. Secur.* 3:262–94
Meier RF, Kennedy LW, Sacco VF. 2001. *The Process and Structure of Crime*. New York: Routledge
Moore T, Clayton R, Anderson R. 2009. The economics of online crime. *J. Econ. Perspect.* 23:3–20
Morris MR, Ryall K, Shen C, Forlines C, Vernier F. 2004. Beyond social protocols: multi-user coordination policies for co-located groupware. In *Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work*, pp. 262–65. New York: ACM
Morris RG. 2011. Computer hacking and the techniques of neutralization: an empirical assessment. In *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, ed. TJ Holt, BH Schell, pp. 1–17. Hershey, PA: IGI Glob.

NCA. 2016. *NCA strategic cyber industry group cyber crime assessment 2016*. NCA Rep., Natl. Crime Agency Strateg. Cyber Ind. Group, London. **http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file**

Ngo F, Paternoster R. 2011. Cybercrime victimization: an examination of individual and situational level factors. *Int. J. Cyber Criminol.* 5:773–93

NIST. 2014. *Framework for improving critical infrastructure cybersecurity*: *version 1.0*. NIST Rep., Natl. Inst. Stand. Technol., Gaithersburg, MD. **https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf**

Ooi KW, Kim SH, Wang QH, Hui KL. 2012. Do hackers seek variety? An empirical analysis of website defacements. In *Proceedings of the 33rd Interanational Conference on Information Systems*, pp. 1–10. Atlanta, GA: AIS

Overvest B, Straathof B. 2015. *What drives cybercrime? Empirical evidence from DDoS attacks*. CPB Disc. Pap. 306, CPB Neth. Bur. Econ. Policy Anal., Hague

Papanikolaou A, Vlachos V, Venieris A, Ilioudis C, Papapanagiotou K, Stasinopoulos A. 2013. A framework for teaching network security in academic environments. *Inf. Manag. Comput. Secur.* 21:315–38

Park JH, Yi KJ, Jeong Y-S. 2014. An enhanced smartphone security model based on information security management system (ISMS). *Electron. Commerce Res.* 14:321–48

Paternoster R, Pogarsky G. 2009. Rational choice, agency and thoughtfully reflective decision making: the short and long-term consequences of making good choices. *J. Quant. Criminol.* 25:103–27

Police Exec. Res. Forum (PERF). 2014. *The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime*. Washington, DC: PERF

Pratt TC, Cullen FT. 2000. The empirical status of Gottfredson and Hirschi's general theory of crime: a meta-analysis. *Criminology* 38:931–64

Priv. Rights Clearinghouse (PRCH). 2017. Privacy rights clearinghouse. *PRCH*. **http://www.privacyrights.org**

Rantala RR. 2008. *Cybercrime against businesses*, *2005*. Bur. Justice Stat. Spec. Rep. NCJ 221943, US Dep. Justice, Washington, DC. **http://www.justiceacademy.org/iShare/Library-BJS/CyberCrimes.pdf**

Reyns BW. 2015. A routine activity perspective on online victimisation: results from the Canadian General Social Survey. *J. Financ. Crime* 22:396–411

Riffkin R. 2014. Hacking tops list of crimes Americas worry about most. *Gallup*, Oct 27. **https://news.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx**

Richards K, LaSalle R, Devost M, van den Dool F, Kennedy-White J. 2017. 2017 cost of cybercrime study. *Accenture*. **https://www.accenture.com/us-en/insight-cost-of-cybercrime-2017**

Rogers RW. 1975. A protection motivation theory of fear appeals and attitude change. *J. Personal.* 91:93–114

Rogers MK. 2006. A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digit. Investig.* 3:97–102

Sampson RJ. 2012. *Great American City*: *Chicago and the Enduring Neighborhood Effect*. Chicago: Univ. Chicago Press

Sampson RJ, Laub JH. 1993. *Crime in the Making: Pathways and Turning Points Through Life*. Cambridge, MA: Harvard Univ. Press

Schell BH, Dodge JL. 2002. *The Hacking of America*: *Who's Doing It*, *Why*, *and How*. Westport, CT: Greenwood Publ.

Scott MS. 2003. *The Benefits and Consequences of Police Crackdowns*. Washington, DC: Off. Comm. Oriented Polic. Serv.

Seebruck R. 2015. A typology of hackers: classifying cyber malfeasance using a weighted arc circumplex model. *Digit. Investig.* 14:36–45

Short JF. 1998. The level of explanation problem revisited: the American Society of Criminology 1997 presidential address. *Criminology* 36:3–6

Siponen M, Pahnila S, Mahmood MA. 2010. Compliance with information security policies: an empirical investigation. *Computer* 43:64–71

Siponen M, Vance A. 2010. Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Q.* 34:487–502

Siponen M, Willison R. 2009. Information security management standards: problems and solutions. *Inf. Manag.* 46:267–70

Skinner WF, Fream AM. 1997. A social learning theory analysis of computer crime among college students. *J. Res. Crime Delinquency* 34:495–518

Sloan-Howitt M, Kelling GL. 1990. Subway graffiti in New York City: Gettin' up versus meanin' it and cleanin' it. *Secur J.* 1:131–36

Spano R, Freilich JD. 2009. An assessment of the empirical validity and conceptualization of individual level multivariate studies of lifestyle/routine activities theory published from 1995 to 2005. *J. Crim. Justice* 37:305–14

Steinmetz KF. 2015. Craft(y)ness: an ethnographic study of hacking. *Br. J. Criminol.* 55:125–45

Stockman M, Heile R, Rein A. 2015. An open-source honeynet system to study system banner message effects on hackers. In *Proceedings of the 4th Annual ACM Conference on Research in Information Technology*, pp. 19–22. New York: ACM

Storm D. 2015. MEDJACK: hackers hijacking medical devices to create backdoors in hospital networks. *Computerworld*, June 8. **https://www.computerworld.com/article/2932371/cybercrime-hacking/medj1ack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html**

Sykes GM, Matza D. 1957. Techniques of neutralization: a theory of delinquency. *Am. Sociol. Rev.* 22:664–70

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

Testa A, Maimon D, Sobesto B, Cukier M. 2017. Illegal roaming and file manipulation on target computers. *Criminol. Public Policy* 16:689–726

Torres JM, Sarriegi JM, Santos J, Serrano N. 2006. Managing information systems security: critical success factors and indicators to measure effectiveness. In *International Conference on Information Security*, pp. 530–45. Berlin: Springer

Tseloni A, Mailley J, Farrell G, Tilley N. 2010. Exploring the international decline in crime rates. *Eur. J. Criminol.* 7:375–94

Valnour. 2009. Revenge is a dish best served cold. *Hacker Q.* 26:32

Van Wilsem J. 2013. Hacking and harassment—do they have something in common? Comparing risk factors for online victimization. *J. Contemp. Crim. Justice* 29:437–53

Waldrop MM. 2016. How to hack the hackers: the human side of cybercrime. *Nature* 533:164–67

Wall DS. 2001. *Crime and the Internet*. New York: Routledge

Wall DS. 2007. Policing cybercrimes: situating the public police in networks of security within cyberspace. *Police Practice Res.* 8:183–205

Wall DS. 2013. Enemies within: redefining the insider threat in organizational security policy. *Secur. J.* 26:107–24

Wang J, Gupta M, Rao HR. 2015. Insider threats in a financial institution: analysis of attack-proneness of information systems applications. *MIS Q.* 39:91–112

Wilbur KC, Zhu Y. 2009. Click fraud. *Mark. Sci.* 28:293–308

Wilcox P, Cullen FT. 2018. Situational opportunity theories of crime. *Annu. Rev. Criminol.* 1:123–48

Wilson T, Maimon D, Sobesto B, Cukier M. 2015. The effect of a surveillance banner in an attacked computer system: additional evidence for the relevance of restrictive deterrence in cyberspace. *J. Res. Crime Delinquency* 52:829–55

Willison R, Siponen M. 2009. Overcoming the insider: reducing employee crime through Situational Crime Prevention. *Commun. ACM* 52:133–37

Wolfe SE, Higgins GE, Marcum CD. 2008. Deterrence and digital piracy: a preliminary examination of the role of viruses. *Soc. Sci. Comput. Rev.* 26:317–33

Workman M, Bommer WH, Straub D. 2008. Security lapses and the omission of information security measures: a threat control model and empirical test. *Comput. Hum. Behav.* 24:2799–816

Yar M. 2005. The novelty of cybercrime: an assessment in light of routine activity theory. *Eur. J. Criminol.* 2:407–27

Yip M, Shadbolt N, Webber C. 2013. Why forums? An empirical analysis into the facilitating factors of carding forums. In *Proceedings of the 5th Annual ACM Web Science Conference*, pp. 453–62. New York: ACM

Young R, Zhang L, Prybutok VR. 2007. Hacking into the minds of hackers. *Inf. Syst. Manag.* 24:281–87
Yu S. 2014. Fear of cyber crime among college students in the United States: an exploratory study. *Int. J. Cyber Criminol.* 8:36–46
Yucedal B. 2010. *Victimization in cyberspace: an application of Routine Activity and Lifestyle Exposure theories*. PhD Diss., Kent State Univ., Kent, OH
Zimring WD. 2006. *The Great American Crime Decline*. New York: Oxford Univ. Press