Security Journal
https://doi.org/10.1057/s41284-020-00282-y

ORIGINAL ARTICLE

Examining the crime prevention claims of crime prevention through environmental design on system-trespassing behaviors: a randomized experiment

Daren Fisher[1] · **David Maimon**[2] · **Tamar Berenblum**[3]

Accepted: 31 December 2020

Abstract

Crime prevention through environmental design (CPTED) is a non-punitive method for reducing crime through the design of the built environment. The relevance of CPTED strategies, however, is less clear in the context of computing environments. Building upon prior research indicating that computing environments may change computer users' behaviors, this study tests the effectiveness of CPTED-based approaches in mitigating system-trespassing events. Findings from this randomized controlled field trial demonstrate that specific CPTED strategies can mitigate hacking events by reducing the number of concurrent activities on the target computer, attenuating the number of commands typed in the attacked computer, and decreasing the likelihood of hackers returning to a previously hacked environment. Our findings suggest some novel and readily implemented strategies for reducing cybercrime.

Keywords CPTED · Cybercrime · Hacking · Crime prevention · Randomized experiment

Introduction

For centuries, societies around the globe have developed design features to make crime harder to commit, limit criminal opportunities, and prevent crime (Kitchen and Schneider 2007). It is now routine to design and build the physical environment to provide safer spaces for human interaction (Cozens and Love 2015), as

✉ Daren Fisher
dfisher3@citadel.edu

[1] Department of Criminal Justice, The Citadel, Capers Building 330, 171 Moultrie Street, Charleston, SC 29409, USA

[2] Department of Criminal Justice and Criminology and Department of Computer Science, Georgia State University, Atlanta, USA

[3] Cyber Security Research Center (H-CSRC), The Hebrew University, Jerusalem, Israel

Published online: 29 January 2021

criminologists, planners, and architects create areas that are conducive to 'non-problematic' activity while simultaneously discouraging crime and disorderly behavior under the banner of crime prevention through environmental design (CPTED) (Sutton et al. 2008, p. 60). Drawing upon more than half a century of insights (see Jacobs 1961), there is now "little doubt" that CPTED can influence offender decision making (Armitage et al. 2018, p. 123). Numerous governments and the United Nations (2007) have shared this position and have implemented CPTED techniques across North America, the Middle East, Europe, and Australasia (Ekblom et al. 2013; Cozens and Love 2015).

The relevances of CPTED strategies are less clear in the context of hacked computing environments, however. Hacking or cracking is commonly defined as the unauthorized access of a computer system with criminal intention (Grabosky 2016). Acknowledging the potential risks and damages that these crimes pose to governmental, private, and business organizations, many official efforts have been devoted to the development of technical tools like anti-malware software, vulnerability scanners, firewalls, and Intrusion Detection/Prevention Systems (Bace and Mell 2001). Sharing similarities with terrestrial impediments to crime, these interventions aim to identify and alert for vulnerabilities and prevent the development of cyber-attacks (Waldrop 2016). Although these tools are designed to identify vulnerabilities and prevent their exploitation by malicious actors, none of these tools allow complete prevention and rapid detection of these incidents as well as effective mitigation of the consequence of an attack. To this point, few prior studies have explored the way that different configurations of an attacked computing environment influence the behaviors of illegitimate users of the system (see Testa et al. 2017; Wilson et al. 2015; Maimon et al. 2014), with no prior research having investigated the effectiveness of CPTED approaches in preventing and mitigating the development of hacking events.

Utilizing recent advances in cybercrime research, we designed the present study to extend the experimental research on CPTED and to observe whether its benefits extend to online environments. Cyberspace is an ideal place to examine criminological theories that are unable to be tested in the terrestrial world as cybercrime seems to follow similar offending patterns which have been observed in offline environments (Leukfeldt and Yar 2016; McGuire 2007; Yar 2005). As computer environments are able to be identically duplicated and are able to be manipulated for remote hackers (Farinholt et al. 2002; Spitzner 2003), this study leverages these previous insights to provide the cleanest conceptual test of CPTED that has been completed and tests four potential methods for reducing cybercrime. By randomly assigning offenders to identical environments and observing their behavior within these environments over a period of 30 days, this study examines whether interventions modeled after the CPTED concepts of territoriality, surveillance, access control, and place management (Sohn 2016; NSW Department of Urban Affairs and Planning 2001) were able to reduce hacking behaviors.

Theoretical background

Crime prevention through environmental design

CPTED rests upon the claim that "the proper design and effective use of the built environment can lead to a reduction in the fear and incidence of crime, and an improvement in quality of life" (Crowe 2000, p. 46). Beginning with the seminal works of Jacobs (1961), Jeffery (1977), and Newman (1972), this multidisciplinary approach to crime prevention draws upon insights from criminology, environmental psychology, planning, and architecture to achieve these goals (Cozens 2008). This approach to crime prevention hypothesizes that through changing a potential offender's perception of a place crime can be reduced (Brantingham et al. 1991; Cozens et al. 2005). Recognizing that certain environmental designs unintentionally lead to the commission of crime and social decay (Giles-Conti et al. 2016; Haider and Iamtrakul 2018; Gotham and Kennedy 2019), the core of this approach to crime prevention is identifying what *does* work instead of what *ought* to work (Jacobs, 1961; Cherney and Sutton 2007).

Empirically identifying what *does* work has however been "as difficult as untangling a spider's web" for both practical and theoretical reasons (Kitchen and Schneider 2004, p. 158). CPTED is primarily rooted in rational choice theories of crime (Cozens 2008). Beyond this underlying assumption, greater agreement in core concepts has proven more difficult. Driven in part by continued disciplinary disputes between planners, urban designers, police, and criminologists (Zahm 2005), numerous typologies have emerged that identify anywhere from four to 21 principles of CPTED across one to three strata. Moffat (1983) has suggested that there are six core CPTED domains,[1] whereas those such as Cozens (2014) have provided multilevel integrated models composed of 21 principles across three strata.[2] While more theoretically plausible and encompassing, more complex CPTED theories have been attributed in part as leading to inconsistent applications and transferability issues across contexts (Gibson and Johnson 2016; Ekblom 2011). In practice, Sohn (2016) argues that the four key principles of CPTED that have emerged are (1) territoriality, (2) surveillance, (3) place management, and (4) access control. This more parsimonious approach has been embraced legislatively and employed routinely in numerous jurisdictions, including the Australian state of New South Wales since 2001 (Clancey et al. 2016; NSW Department of Urban Affairs and Planning 2001) and provides an ideal place to begin developing the randomized experimental literature on CPTED.

Despite enjoying widespread political support as a theoretically non-punitive crime prevention option (Fisher and Piracha 2012), CPTED's effectiveness at preventing crime has been questioned. While extensive, the current evidence base

1 According to Moffat (1983), the six core 1st-generation CPTED domains are territoriality, surveillance, target hardening, access control, image maintenance, and activity program support.

2 The three strata are 1st-generation CPTED, 2nd-generation CPTED, and Surrounding Environment/Routine Activities. For a full description see Cozens (2016).

has been unable to isolate the impacts of design interventions on crime from idiosyncratic environmental factors (Cozens and Love 2015; Taylor 2002). CPTED has also proven to be difficult to implement effectively in practice. Driven by the vague definitions within the literature and divergence between its intended use and actual implementation, Ekblom (2011) presents that CPTED strategies have led to wasted time, resources, and effort (see also Minnery and Lim 2005; Parnaby 2006). CPTED, thus, requires careful and long-term coordination between numerous stakeholder groups to mitigate its risks to the public regardless of its potential crime prevention benefits (Clancey et al. 2014). Spurred on by these observations and Zahm's (2005, p. 291) dictum that "without evaluation, it will never be clear when, where, and why such programs have been effective," recent studies have collected innovative data to address the empirical gap in the CPTED literature. These studies have produced supporting evidence that CPTED can reduce robberies and burglaries (Armitage et al. 2018; Casteel and Peek-Asa 2000; Peeters and Berken 2017), residential crime (Sohn 2016), and crime within schools (Vagi et al. 2018). While these studies represent a small fraction of the implementations of these principles globally, raising concerns regarding how indicative these experiences are, they do demonstrate that when implemented and maintained well CPTED initiatives can reduce crime across a wide range of locations.

Compounding previous criticisms, the empirical literature underpinning our understanding of the crime prevention benefits of CPTED is still underdeveloped. In examining whether one is able to link causally CPTED to crime reductions, Taylor (2002) neatly presents three major issues that have limited the inferences from previous studies and need to be overcome. First, the majority of the empirical evidence-testing CPTED has been cross-sectional due to the cost-intensive nature of implementing CPTED interventions and measuring crime over time (Taylor 2002). As crime is neither stable over time nor equal across places, such cross-sectional studies are unable to assess the temporal ordering of any relationships or any relative impacts on crime (Bowen and Wiersma 1999). Connected to this point, Taylor (2002) also laments that the lack of resources devoted to studying these impacts has rendered it difficult to gain the required statistical power to allow researchers to detect any impacts stemming from the implementation of any CPTED (see also Armitage and Monchuk 2011). Finally, and most difficult to overcome, Taylor (2002, p. 416) presents that in gaining the statistical power capable of detecting any impacts, heterogeneity in treatment and "selection problems make it exceedingly difficult to separate qualities of locale from qualities of those drawn to the locale." Unlike the previous two issues, the inability to distinguish the effects of treatment from idiosyncratic factors in the terrestrial environment persists regardless of the sample size and the length of the observation period. Paradoxically, the larger the sample size and observation period, the less likely any impacts will be able to be observed (Weisburd et al. 1993; Sherman 2007). This challenge, thus, cannot be solved through increased research resources, and instead alternative research methods are required to better identify the crime prevention benefits of CPTED.

To date, only two existing studies can be classified as level 3 studies (Crow and Bull 1975; Eck and Wartell 1996; see Cozens and Love 2015) according to the Maryland Scale (Farrington et al. 2002). A level 3 study according to the Maryland scale includes a study design where a comparison is made between two or more comparable units of analysis, one with and one without the program or intervention. Drawing upon the assertions of Cook and Campbell (1979), Farrington et al. (2002, p. 17) state that this should be regarded “as the minimum design that is adequate for drawing conclusions about what works.” Although studies that meet this standard are unable to account for selection effects, level 3 studies are able to account for maturation and trend influences (Farrington et al. 2002). Since the observations of Cozens and Love (2015) there have been some key developments where linear regression methods and structural equation modeling have been used to enhance previous cross-sectional case study, and before-and-after differences (see Armitage et al. 2018; Casteel and Peek-Asa 2000; Peeters and Berken 2017; Sohn 2016; Vagi et al. 2018). These methods have been better able to account for previously unmeasured contextual and individual factors, potentially yielding a Maryland Scale rating of 4 whereby they deal with selection and extraneous factors more adequately. Given the findings across these studies that support CPTED’s crime reduction claims, there is growing evidence that CPTED is able to influence offender decisions (Armitage et al. 2018). However, the need to produce stronger evidence investigating its crime prevention tag remains.

On the relevance of CPTED in the design of secure cyber environments

Cyber environments are important domains within which online criminal activity takes place. Originally designed for supporting efficient information exchange between remote individuals and organizations in cyberspace, these online environments now facilitate ground for the rise in the volume of cybercrime incidents around the world (Broadhurst 2006), costing in excess of $600 billion globally in 2017 (Lewis 2018). Indeed, the consequences of recent data breach to several major financial, communication, and insurance companies computing environments have been broad and consequential for nations and thousands of people (Holt and Bossler 2014). Many traditional criminal justice policies for reducing cybercrime have, thus, far proven ineffective, as sanction threats are unlikely on their own to influence offending behavior (Mayer 2015; Kigerl 2016). Hackers are generally aware that it is unlikely that they will be identified due to their use of proxies (Geers 2010), and even if they are identified, many nations will not extradite their own citizens (Brenner 2009). Coupled together, these factors display the futility of traditional criminal justice responses for incapacitating or deterring these offenders (Holt 2017).

Still**,** the virtual environment shares many similarities with the terrestrial world, especially with regard to criminality. Numerous studies have found that virtual and terrestrial criminality share numerous practical and theoretical components (Donner et al. 2014; Yar 2005), supporting Grabosky’s (2001, p. 243) claim that “virtual criminality is basically the same as the terrestrial crime with which we are familiar.” Online environments also face many criminal challenges that are similar to public spaces. Businesses and public spaces in both realms seek to attract legitimate and law-abiding users while discouraging criminal behavior (Atlas 2008). Particularly with regard to cyber trespassing, "crossing boundaries into other people's property and/or causing damage" (Yar 2005, p. 410), the goals of crime prevention in both domains are practically identical.

In light of recent criminological interventions displaying the ability to reduce and mitigate cyber trespassing (Testa et al. 2017; Wilson et al. 2015; Maimon et al. 2014; Maimon and Louderback 2019), the experiences of CPTED in preventing terrestrial trespassing holds promise for providing a range of techniques for producing cybersecurity methods (Whitford 2018). For example, Maimon and colleagues (2014) and Stockman and colleagues (2015) tested the effect of a warning banner in an attacked computer system on the progression, frequency, and duration of system-trespassing events and found that the warning resulted in a shorter average duration of the system-trespassing incidents (interestingly, the effect of a warning message on the duration of repeated trespassing incidents was attenuated in computers with a large bandwidth capacity). Wilson and associates (2015) assessed the effect of a surveillance banner on the probability of commands being entered in the attacked computer system. 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 initial system-trespassing incidents. Finally, Maimon and Louderback (2019) investigated whether the level of ambiguity regarding the presence of surveillance in an attacked computer system influences system trespassers' likelihood to clean their tracks during the progression of an event. Their findings indicate that the presence of unambiguous signs of surveillance (i.e., the presence of both a surveillance banner and program in the attacked system) increases the probability of clean tracks commands being entered on the system.

Indeed, extensive research has revealed that prominent criminological theories have explanatory value for cybercrime. This evidence has been especially forthcoming when testing theories that have underlying assumptions of rational offenders including self-control (Donner et al. 2014; Holt et al. 2012; Holtfreter et al. 2008), routine activities theory (Leukfeldt and Yar 2016; Navarro and Jasinki 2013; Ngo and Paternoster 2011; Maimon et al. 2014), and restrictive deterrence (Testa et al. 2017; Wilson et al. 2015; Maimon et al. 2014). Far from suggesting that cybercrime is discontinuous from the terrestrial world as Capeller (2001) argues, these studies demonstrate the value of criminological theories and suggest a range of policy alternatives that can address cybercrime beyond formal sanctioning. Employing techniques derived from criminological approaches, scholars have revealed a growing number of policies that hold promise for reducing system-trespassing incidents, including warning and surveillance banners, as well as surveillance software installed on an attacked system (Testa et al. 2017; Wilson et al. 2015; Maimon et al. 2014). Taken together, there is a burgeoning evidence base that indicates that various configurations of computing environments may result in reduction of cybercrime events within targeted online environments. Still, only few studies have investigated the effectiveness of CPTED strategies in influencing hackers' online behaviors.

Present study

In an effort to bridge this empirical gap, this study investigates the effect of four CPTED approaches—territoriality, surveillance, place management, and access control (Sohn 2016; NSW Department of Urban Affairs and Planning 2001) on system trespassers' online behaviors during the progression of system-trespassing event. Below, we provide a brief conceptual overview of each of the four CPTED techniques that we are focusing on, and detail how each technique could shape the system trespassers' initiation of those activities while working with an attacked system.

Territoriality

The concept of territoriality stems from the observation that the physical design of a space can extend a sphere of influence over those in contact with it (Shah and Kesan 2007). Territorial reinforcement helps approved users to develop a sense of proprietorship and ownership and can conversely discourage illegitimate users (Carter et al. 2003). Territoriality requires creating and maintaining spatial hierarchies, and ensuring that clear, well-recognized boundaries exist between public and private areas (Sutton et al. 2008). These barriers may include hedges and walls between public and private areas, street signs, and vegetation or changes in surface that are used to indicate zones of transition from private to public space (Atlas 2008). Through clearly indicating borders in the physical environment, it is easier for residents and other authorized people to legitimately challenge individuals who seem to be trespassing or misusing a space and also promotes a greater perception of risk by offenders (Crowe 2000, p. 37). In line with the concept of territoriality, branding, signposts, and other reminders are routinely used online to remind legitimate and illegitimate users of ownership and influence online behavior (van den Bos and Nell 2006), we suspect that notifying hackers that they had entered into a protected online environment will instigate less activity on behalf of the trespassers during the progression of the event (i.e., lower number of concurrent open terminals and fewer commands typed), and reduce the likelihood of repeated system-trespassing events.

Surveillance

Building upon on Jacobs' (1961) 'eyes on the street' principle, surveillance aims to increase the perceived risks associated with offending by increasing the perception that all actions in a space will be observed (Sutton et al. 2008, p. 63). Through perceptually increasing the potential for intervention, apprehension, and prosecution, rational offenders would thus be less inclined to break the law (Atlas 2008). This may be achieved through informal means that utilize casual observation from the people that use a space, or through formal means that exist in the form of organized guardianship from people (civilians, security guards, and staff) and technology (CCTV) (Sutton et al. 2008). The positions of paths, shops, and houses should be designed so that they can be seen by adjoining users, creating well-lit areas, and having activity generators and facilities that increase the use of outdoor spaces (Geason and Wilson 1989). Echoing signs that let people know that their actions are being observed by CCTV and being presented with monitors displaying the footage being captured, we suspect that providing hackers with evidence for the presence of surveillance on the attacked system will lead to less activity on behalf of the trespassers during the progression of the event (i.e., lower number of concurrent open terminals and fewer commands typed), and reduce the likelihood of repeated system-trespassing events.

Place management

Also known as activity, how legitimate activities within the built environment are managed and overseen is important to establishing pride and safety (Sutton et al. 2008). Drawing on reasoning similar to Wilson and Kelling's (1982) Broken Windows Theory, the management and maintenance of the physical environment send cues to those who use a space (Maynard 2004, p. 9). Public places that are broken down, dirty, vandalized, full of rubbish, and generally 'looking unloved' are less likely to encourage active legitimate use by most groups, let alone a sense of pride and ownership by the community (Sutton et al. 2008). Conversely, well-maintained spaces that are well used and well supervised also send out messages to would-be wrongdoers that the community cares (McCamley 2001). These messages are different from surveillance as; while the presence of CCTV or recording one's actions through other electronic means should reduce criminal behavior through increasing the perceived likelihood of observation (surveillance), direct or indirect evidence that there is ownership over the space and someone to take action would be considered place management. Consistent with this, we suspect that presenting trespassers with a banner indicating that the infiltrated infrastructure is cared for and supervised by administrator, will reduce trespassers' activity during the progression of the event through increasing the perceived likelihood of corrective action by the owner of the space (i.e., lower number of concurrent open terminals and fewer commands typed) and reduce the likelihood of repeated system-trespassing events.

Access control

Access control strategies aim to encourage, restrict, and channel activities while denying access to with those who have the potential to commit a crime (Sutton et al. 2008). Like surveillance, access control can involve formal, informal, or mechanical techniques to reach these goals (Sutton et al. 2008). Informal strategies incorporate natural features that change the spatial definition of locations (including gardens and marked entrances that signify moving from public to private areas) (Sutton et al. 2008). Formal access control is more purposeful and is carried out by individuals (security guards and receptionists) or technology (password or key-controlled access points) that can prevent unauthorized access to specific offline or online areas (Atlas 2008). We suspect that requiring users to provide with the login password on random occasions during their work with the system (and after they have logged in) will reduce trespassers' activity during the progression of the event (i.e., lower number of concurrent open terminals and fewer commands typed), and reduce the likelihood of repeated system-trespassing events.

Table 1 below provides a brief summary of the discussion above and example of these four CPTED concepts for ease of reference.

Data and methods

To test whether these interventions could reduce illicit online behavior, we collected unique data that were gathered by a large set of target computers, also known as honeypots (Stoll 1989; Spitzner 2003), built for the sole purpose of being attacked, and deployed on the computer network of a Chinese academic institute. A honeypot is a security resource whose primary value is in being compromised by online offenders in order to allow the collection of data on a hacker's actions with the target of attack (Spitzner 2003). Honeypots provide a number of advantages for ascertain the value of various computing configurations in influencing intruders' behaviors. First, they can be designed to allow all potential attackers to gain access to the system, which is not guaranteed in practice and reduces sample selection bias (Stoll 1989). Second, any system trespassers can also be randomly assigned to an experimental condition, allowing groups receiving different experimental conditions to be directly comparable in expectation. Through removing the idiosyncratic differences between environments and in the application of treatments, cyber environments can be tailored in honeypot experiments to enable criminological theories to be tested (Maimon and Louderback 2019). Indeed, Farrington et al. (2002, p. 17) in their discussion of level 5 studies argue that random assignment to experimental conditions deals with selection effects and provides "the highest possible internal validity." While Berk (2005) and Sampson (2010) note that random experimental designs still suffer from attrition and implementation issues, employing random assignment to experimental conditions provides the opportunity to limit the potential influences stemming from selection effects and, importantly for CPTED, differences in individual treatment conditions.

Despite commonly used by both criminologists (Maimon et al. 2014; Wilson et al. 2015) and computer scientists (Brown et al. 2017) to study online crimes, honeypots do not overcome all methodological challenges, and Holt (2017) raises a number of important considerations and limitations to these methods. While these simulated environments are indistinguishable from normal computers for less sophisticated hackers, fingerprinting[3] techniques can be used by hackers to distinguish between regular online environments and honeypots (Mohammadzadeh et al.

[3] According to Aguirre-Anaya et al. (2014, p. 850), fingerprinting in this context shares similar function to a "biometric fingerprint, where a specific pattern is extracted and compared against a database, the identification of systems is possible due to the different implementations of communication protocols, network services or specific environments. These different features are collected and then a fingerprint is generated, which include enough features to unequivocally identify a specific system of a set of different systems."

Table 1 CPTED definitions and illustrative examples

CPTED concept	Definition	Illustrative examples
Territoriality	Environmental elements that influence users, helping proprietorship for approved users and discouraging illegitimate or criminal actions	Branding, signposts, edges and walls between public and private areas, street signs, vegetation, and changes in surface
Surveillance	Environmental elements that increase the perceived risks associated of offending by increasing the perception that all actions in the environment will be observed and/or recorded	Either casual observation from the people that use a space, and/or formal forms of organized guardianship from people (security guards and staff) and technology (CCTV)
Place management	How legitimate activities within an environment are managed and overseen whereby the management and maintenance of the physical environment sends cues to those using the space	Public activity coordination, site cleanliness, rapid repair of vandalism and graffiti, the replacement of burned out pedestrian and car park lighting, and the removal or refurbishment of decayed parts of the environment
Access control	Environmental elements that encourage, restrict, and channel activities while denying access to with those who have the potential to commit crime	Security guards and receptionists or technology (password or key-controlled access points) that can prevent unauthorized access to specific offline or online areas

2013).[4] In addition, honeypots are able to measure explicit actions but are unable to measure the fundamental attitudes, beliefs, and capabilities of intruders who interact with the honeypot (Holt 2017). Concordantly, while differences between experimental groups are detectable, attributing these differences to unobserved individual-level factors is not possible. Finally, honeypots are also unable to detect communications such as warnings and recommendations between hackers that may alter behavior within a honeypot. As both legal and malicious actors inform one another of weaknesses in computer hardware and software that can be used to harm a system (Holt 2017), the behavior exhibited within a honeypot is not limited to be influenced only by the honeypot itself. As a result, it can be difficult to isolate the mechanisms influencing the actions of hackers within even a completely controlled network.

Still, the usefulness of honeypots in understanding trespassers behaviors persists even after accounting for these limitations. Indeed, a growing body of research suggests that restrictive deterrence and situational prevention techniques are able to influence and in some cases reduce criminal behavior on specific networks (Leukfeldt and Yar 2016; Navarro and Jasinki 2013; Ngo and Paternoster 2011; Bossler and Holt 2009; Testa et al. 2017; Wilson et al. 2015; Maimon et al. 2014). Although these techniques may thus not be able to reduce the total amount of cybercrime on their own, they can thus be used to prevent crime in targeted places. If the goal of an intervention is total protection of a specific location, the ubiquity of opportunities is an asset as even the slightest inconvenience or crime prevention initiative may be enough to demonstrate that other online places are likely to yield results that are more beneficial for crime. While additional challenges can increase the desire to hack these environments (Steinmetz 2015; Holt 2007; Taylor 1999), other prevention techniques that do not increase hacking challenges may still yield crime prevention promise. It is for these situations that crime prevention through environmental design (CPTED) is specifically tailored.

Experimental research design

Unlike common experimental designs that require active subject recruitment, we did not recruit subjects to participate in our experiment. Instead, we deployed our honeypots (which hear forth will be called target computers) on the computer network of a Chinese University between November 6th 2015 and February 24th 2016, and waited for system trespassers to find our systems and employ special software cracking tools to break into them. 100 Public Internet Protocol (IP) addresses were used for the deployment. To simulate a genuine environment, the target computers had a Ubuntu-Linux-based operating system installed on and were modified to reject the

[4] Aguirre-Anaya et al. (2014) also explain several ways that low interaction honeypots could be identified. Huang et al. (2019) also suggest that mid interaction honeypots could be identified by hackers. However, identifying a high interaction honeypots is difficult since all of the function available in a regular computer are available and functionable for attackers to use. Therefore, with high interaction honeypots there is less risk of identifying the honeypots, and concordantly, high interaction honeypots were used in this study.

login attempts by system trespassers on its public IP addresses until a predefined number of attempts (150 + N number) or once a commonly used password which is commonly used by a legitimate user was entered (see https://haveibeenpwned.com/Passwords for a list of most commonly used and owned passwords). Once access to our target computer had been granted, system trespassers were randomly assigned to either the control group or one of the four experiment groups (i.e., a 1 × 5 factorial design). In the first experimental group, *territoriality*, a banner notifying the trespasser that the device infiltrated is owned by the university was presented. In the second experimental condition, *surveillance*, a banner notifying for the presence of surveillance measures on the attacked system was presented to the system trespassers. This banner included also the list of previous (how many) activities that were performed by the trespasses in the system. In the third experimental group, *place management,* a banner indicating that the device was cared for by an administrative person was presented to the system trespasser. Finally, in the last experimental group, access Control, the trespasser was requested to provide the legitimate login credentials in order to escalate privileges on the attacked system. To allow the collection of meaningful data on system-trespassing incidents, we monitored the different components of the system-trespassing incident using specialized software that records the system-trespassing events for later analysis. The collected logs from the servers included all the commands that were entered by the hackers on our servers, as well as the software they downloaded.

Outcome measures

The main unit of analysis for this study is the system-trespassing event. As such, all variables and subsequent analyses are designed to examine how the behavior exhibited by users of each IP address[5] observed on the target computer during a system-trespassing event varies across the CPTED condition that they were exposed to (or the control). To test our hypotheses, we constructed three outcome measures to examine whether each treatment was able to reduce engagement with the target computers (two measures) and reduce the likelihood of subsequent system-trespassing events (one measure). For each of these three outcomes, if the CPTED treatments are successful, then we would expect decrease in each measure relative to the control group. Our first outcome measures the number of concurrent Secure Shell (SSH) sessions/open terminals per unique IP address during a system-trespassing event. All in all, Linux users can control the computer they work with as administrators remotely through a secure shall. Once connected to a computer through SSH, the user can transfer files between the two machines and execute commands on the remote machine. Running concurrent SSH sessions imply increased user activities as more operations could be conducted on the remote computer simultaneously. In line with this rationale, this measure was coded as a count variable, with (1) indicating

[5] An IP address is a unique numeric label (e.g., 131.87.17.67) that identifies specific devices that are connected to a computer network and uses an Internet Protocol (IP) to communicate with other devices (Ruiz-Sánchez et al. 2001).

Table 2 Sample descriptive statistics

Condition	Target computers	Unique IP addresses	Open terminal/ SSH sessions	Commands	China	Ukraine
Control	18	594	1802	994	0.86	0.05
Place management	22	737	1807	824	0.83	0.05
Surveillance	21	561	1554	855	0.83	0.04
Territorial Reinforcement	21	766	2192	1215	0.87	0.04
Access control	18	610	1705	941	0.84	0.05
Total	100	3268	9061	4829	0.85	0.05

a single SSH session originated in a given IP address during a system-trespassing event, and higher numbers represent higher number of concurrent sessions.

Our second dependent variable is the number of commands that were entered in the target computer during the system-trespassing incident.[6] This measure was coded as a count variable, with (0) indicating that no commands were entered from a given IP address after gaining access to the target computers. Finally, our third dependent variable measured as a binary outcome that differentiates between unique IP addresses with more than one recorded trespassing event (1) and IP addresses with only one recorded trespassing incident (0).

Results

Over the 90-day observation period, there were 3,268 IP addresses that instigated 9061 system-trespassing incidents across the 100 target computers. Over the experimental period, all target computers were successfully compromised and experienced a minimum of six system-trespassing events from a minimum of four unique IP addresses. Table 2 provides descriptive statistics of our sample. As can be seen in Table 2, the vast majority of IP addresses used to access these target computers came from China (84.70%), with the second most common country of origin being Ukraine (4.53%). Further indicating that there was meaningful variation across the treatment conditions, the number of sessions recorded in each condition ranged from a minimum of 1554 (surveillance) to a maximum of 2192 (territorial reinforcement).

[6] It should be noted that a very efficient hacker will be able to obtain their goals with fewer commands. However, to accomplish these goals, the hacker will first need to understand the system they are working within. System configuration and the computing environment may influence the progression of the criminal event and the volume of engagement with the system (see Wilson et al. 2015). As such, one would expect if the treatment had its desired impact, then we would see fewer commands, but if it is not effective then it would likely lead to more in order to navigate the additional elements compared to the control group.

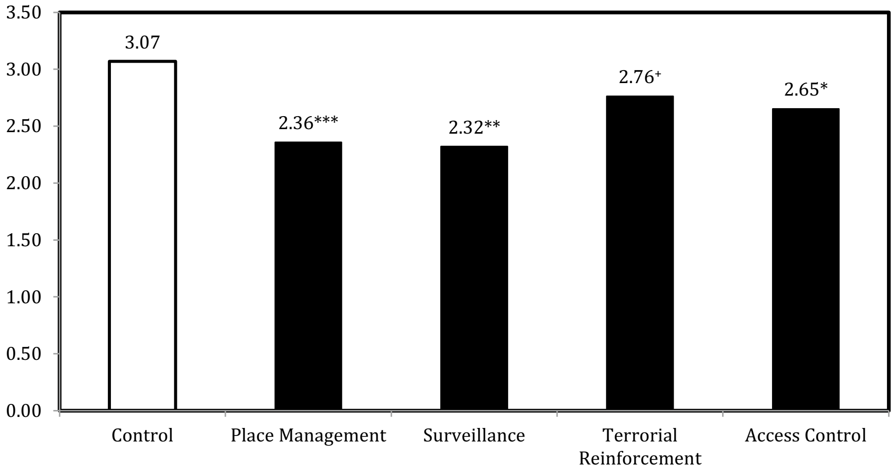

Fig. 1 Average number of concurrent open terminals (SSH sessions) per unique IP address ($p<0.1^{+}$, $p<0.05$*, $p<0.01$**, $p<0.001$*)

Number of concurrent SSH sessions

The findings from this experiment indicated that all experimental conditions experienced numerically fewer average SSH sessions per IP address compared to the control group ($F=1.97$, $p=0.105$). As can be seen in Fig. 1, the control group experienced an average of 3.07 concurrent SSH sessions per IP address during the observation window. While the reduction in average number of concurrent SSH sessions was marginally statistically significant for territoriality ($t=-1.407$, $p=0.087$), it was statistically significant for the place management ($t=-4.471$, $p<0.001$), surveillance ($t=-3.127$, $p=0.003$), and access control conditions ($t=-1.848$, $p=0.042$). These findings suggest that all four CPTED interventions have the potential to reduce the number of concurrent SSH sessions in an online environment even after a computer has been illegally accessed.

Command usage

Across the entire sample, the number of commands that were used after gaining access the system was 1.48, and a maximum number of 71 commands were observed for a single IP address across 78 sessions. The highest number of commands that were used within a single SSH session was seven, with 2517 sessions elapsing without a single command being entered. The control group (0.80) and the place management condition (0.81) had the highest proportion of SSH sessions without a command, with the access control ($t=2.748$, $p=0.006$) and territoriality conditions ($t=2.322$, $p=0.02$) having statistically significant more SSH sessions with at least one command. When the average number of commands in each experimental condition was examined, both the access control and territoriality conditions

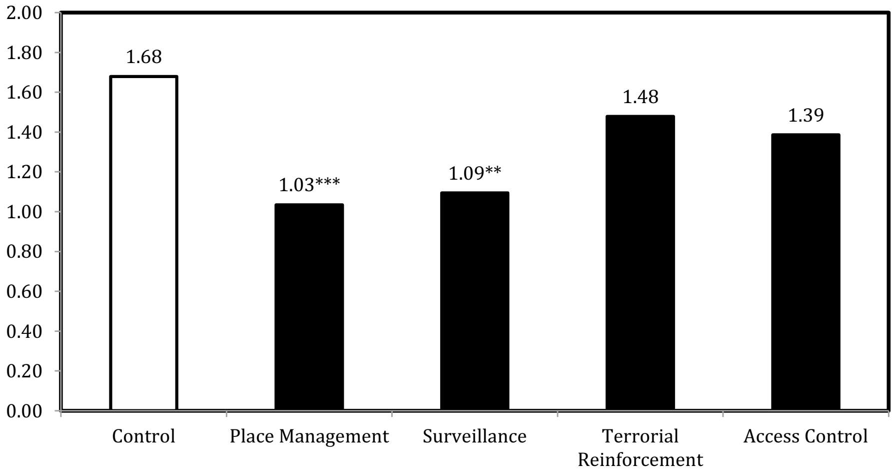

Fig. 2 Average number of commands entered per unique IP address ($p < 0.1^{+}$, $p < 0.05^{*}$, $p < 0.01^{**}$, $p < 0.001^{***}$)

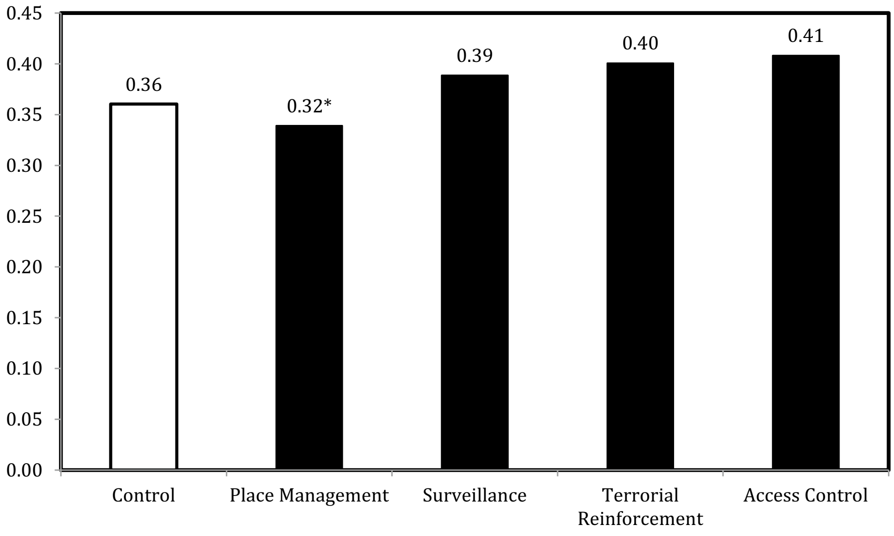

Fig. 3 Proportion of unique IP addresses that returned for more than one session ($p < 0.05^{*}$)

were statistically indistinguishable from the control group, however (see Fig. 2). The place management ($t = -4.765$, $p < 0.001$) and surveillance ($t = -2.593$, $p = 0.008$) conditions did, however, yield reductions in the average number of commands that were used compared to the control group. Taken to together these findings suggest that despite some interventions making it more that a system trespasser would input a command, the net impact on the number of commands was either null (territoriality and access control) or resulted in reductions in the average number of commands that were used (Fig. 3).

The most frequently used command was *wget*, which was used 4472 times across the experiment. This command is used to retrieve content from a server and was used for an average of 1.56 times per unique IP address within the control group. This average dropped to 1.045 for the place management condition ($t = -18.87$, $p < 0.001$), 1.40 for the place management condition ($t = -5.22$, $p < 0.001$), 1.47 for the place management condition ($t = -2.97$, $p = 0.003$), and 1.42 for the place management condition ($t = -4.68$, $p < 0.001$). The next most frequently used commands were *ps* ($f = 53$) and *kill* ($f = 43$), which display the currently running processes and stop currently running processes, respectively. Place management was the only experimental condition that saw a reduction in the use of the *ps* command, which was only used by 0.7% of unique IP addresses ($t = -9.52$, $p < 0.001$). Opposite to predictions, however, the surveillance, territorial reinforcement, and access control groups had numerically more uses of the *kill* command than the control group. However, IP addresses exposed to the place management command did see less use of the *kill* command ($t = -9.52$, $p < 0.001$).

Likelihood of returning

Our last hypothesis that this study examined was whether any of the treatment conditions made system trespassers less likely to return to the target computer. Across the entire sample, 35.01% ($f = 200$) of unique IPs returned to the target computer after concluding their first SSH session in a different time. Contrary to expectation, the territoriality and access control groups produced a numerically greater proportion of unique IPs that returned to a target computer compared to the control group. These differences were not found to be statistically significant using one- or two-tailed hypothesis tests, however. The only statistically significant difference that was detected was for the place management condition ($t = -1.652$, $p = 0.049$). While the proportion for the surveillance group (0.3224) was nearly identical to the place management group (0.3213), this difference coupled with the slightly smaller sample size was sufficient to yield a statistically null difference ($p = 0.176$).

Discussion

CPTED offers a range of non-punitive methods for reducing crime through the purposeful design of environments, and the findings from this study suggest that this is not limited solely to terrestrial environments. This study sought to examine whether a range of techniques driven by the CPTED principals from the longest continuously used guidelines from Australia (Clancey et al. 2016) were able to mitigate system-trespassing behavior in an experimental setting. Across all three outcomes, the findings from this study displayed that CPTED techniques were able to alter behavior of system trespassers in an online environment. These findings provide further credence that the impacts of CPTED are not just limited to establishing "fortress-like structures" (see Currie 1993) and can be leveraged in broader and more social settings (Reynald 2011). Particularly as human action and crime becomes increasingly prevalent within online environments (Chen et al. 2017), these findings suggest that the benefits of this approach to crime prevention extend into online domains as well. Extending the previous empirical literature on CPTED, these findings also demonstrate that the four interventions examined were able to reduce offending behavior within an experimental setting. Specifically, this addresses the issue in previous studies that were unable to isolate the impacts of design interventions on crime from idiosyncratic environmental factors (see Cozens and Love 2015; Taylor 2002). While this remains to be replicated within a terrestrial study, this study does provide support to the evidence base that previously observed crime prevention benefits exist regardless of idiosyncratic differences across treatments.

Consistent with previous studies (see Testa et al. 2017; Wilson et al. 2015; Maimon et al. 2014, 2019) and boarder experiences with CPTED (Fisher and Piracha 2012; Cozens and Love 2015; Clancey et al. 2016), none of the interventions were able to stymie all illegal actions and achieve absolute prevention. While this is unsurprising given that the interventions were only introduced after the initial crime of system trespassing, these techniques were able to mitigate the actions of hackers within compromised computer systems. It should be noted that the impacts were limited and did not extend to all experimental conditions. Across all three outcomes, both the place management and surveillance interventions performed better than territoriality and access control conditions. Further, other indicators including the likelihood of returning for additional system-trespassing session suggested that these two conditions had the potential to perform worse than even the control group. The only condition that reduced the likelihood of returning was place management. Particularly as this was the only condition that indicated active human engagement, this study highlights that future research focuses upon other CPTED interventions that rely more upon potential human presence than upon technological presence. Particularly as all other experimental groups either had automated processes or were passive in nature, this marks a key departure for this CPTED technique from the others that were observed.

Despite these strengths, this study highlights the need for replication. As discussed above, there is a need to examine different CPTED interventions. While this study focused upon the four core techniques highlighted by the NSW Department of Urban Affairs and Planning (2001), many additional techniques beyond these warrant their own examination. In addition, the interventions themselves only represent one method for designing a crime prevention strategy in line with these principles. As such, this study highlights that other techniques may have additional value within the domains explored in this study and beyond. In addition, as this study was unable to observe the interpretation of these cues, it would be of great empirical benefit for subsequent studies (especially qualitative studies) to further examine the mechanisms underlying the impacts of these experimental conditions compared to the control group. Although this study was conducted online and theoretically limited the impact of the physical world, as the study was conducted at a Chinese institution and the majority of system trespassers did use a Chinese IP address, this study highlights the need for replication in other nations to better evaluate the generalizability of these findings. Finally, as this study was limited an observation period of 30 days, this study highlights the need for future studies to examine whether the impacts observed here persist over time, spread, or potentially decay (see Sherman 1990; Nagin 1998; Sorg et al. 2017).

Taking these limitations into consideration, we hope that our findings may support existing contemporary cybersecurity efforts which are aimed at mitigating attackers' actions while exploiting vulnerabilities and working with an attacked platform in a more efficient way. 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 that are designed to prevent system trespassing from developing (Waldrop 2016). Unfortunately, only negligent number of tools support effective mitigation of the consequence of an attack. One major reason for the deficiency of these tools in accomplishing these goals is their failure to integrate knowledge about online attackers' behaviors in response to different configurations of the attacked computer system during the progression of the system-trespassing event. This study brings context embedded experimental evidence regarding computing environments that entice attackers to behave in a predictable manner, which in turn, may result in less severe consequences to the attacked system.

Conclusions

Findings from this study demonstrate that specific CPTED strategies can prevent crime after removing the influence of idiosyncratic differences. These findings thus not only provide evidence for the value of this crime prevention perspective but also demonstrate that it has value beyond the physical built environment. In addition, the techniques used in this experiment provide an easily implement means for minimizing illegal online behavior by reducing the number of hacking sessions, the number of commands typed in the attacked computer, and the likelihood of hackers returning to a previously hacked environment.

Compliance with ethical standards

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

Aguirre-Anaya, E., G. Gallegos-Garcia, N. Solano Luna, and L.A. Villa Vargas. 2014. A new procedure to detect low interaction honeypots. *International Journal of Electrical & Computer Engineering* 4 (6): 848–857.

Armitage, R., C. Joyce, and L. Monchuk. 2018. Crime Prevention Through Environmental Design (CPTED) and retail crime exploring offender perspectives on risk and protective factors in the design and layout of retail environments. In *Retail Crime*, 123–154. Cham: Palgrave Macmillan.

Armitage, R., and L. Monchuk. 2011. Sustaining the crime reduction impact of designing out crime: Re-evaluating the secured by design scheme 10 years on. *Security Journal* 24 (4): 320–343.

Atlas, R.I. 2008. Understanding CPTED and situational crime prevention. In *21st century Ssecurity and CPTED*, 62–87. Boca Raton: Auerbach Publications.

Bace, R., and P. Mell. 2001. *NIST special publication on intrusion detection systems*. Mclean Va: Booz-Allen and Hamilton Inc.

Berk, R.A. 2005. Randomized experiments as the bronze standard. *Journal of Experimental Criminology* 1 (4): 417–433.

Bossler, A.M. 2017. Need for debate on the implications of honeypot data for restrictive deterrence policies in cyberspace. *Criminology & Public Policy* 16 (3): 681–688.

Bossler, A.M., and T.J. Holt. 2009. On-line activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology* 3 (1): 400–420.

Bowen, H.P., and M.F. Wiersema. 1999. Matching method to paradigm in strategy research: Limitations of cross-sectional analysis and some methodological alternatives. *Strategic Management Journal* 20 (7): 625–636.

Brantingham, P.L., P.J. Brantingham, and P.S. Wong. 1991. How public transit feeds private crime: Notes on the Vancouver 'Skytrain'experience. *Security Journal* 2 (2): 91–95.

Brenner, S.W. 2009. *Cyberthreats: The emerging fault lines of the nation state*. Oxford: Oxford University Press.

Broadhurst, R. 2006. Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management* 29 (3): 408–433.

Brown Farinholt, Mohammad Rezaeirad, Paul Pearce, Hitesh Dharmdasani, Haikuo Yin, Stevens Le Blond, Damon McCoy, Kirill Levchenko. 2017. *To Catch a Ratter: Monitoring the Behavior of Amateur DarkComet RAT Operators in the Wild*, In *Proceedings of the 38th IEEE Symposium on Security and Privacy (Oakland)*, San Jose, CA.

Capeller, W. 2001. Not such a neat net: Some comments on virtual criminality. *Social & Legal Studies* 10 (2): 229–242.

Carter, S.P., S.L. Carter, and A.L. Dannenberg. 2003. Zoning out crime and improving community health in Sarasota, Florida: "Crime prevention through environmental design." *American Journal of Public Health* 93 (9): 1442–1445.

Casteel, C., and C. Peek-Asa. 2000. Effectiveness of crime prevention through environmental design (CPTED) in reducing robberies. *American Journal of Preventive Medicine* 18 (4): 99–115.

Chen, H., C.E. Beaudoin, and T. Hong. 2017. Securing online privacy: An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior* 70: 291–302.

Cherney, A., and A. Sutton. 2007. Crime prevention in Australia: Beyond 'what works?' *Australian & New Zealand Journal of Criminology* 40 (1): 65–81.

Clancey, G., D. Fisher, and A. Rutherford. 2014. An exploratory study of crime risks and the planning process. *Crime Prevention and Community Safety* 16 (1): 1–19.

Clancey, G., D. Fisher, and N. Yeung. 2016. A recent history of Australian crime prevention. *Crime Prevention and Community Safety* 18 (4): 309–328.

Coleman, R., S. Tombs, and D. Whyte. 2005. Capital, crime control and statecraft in the entrepreneurial city. *Urban studies* 42 (13): 2511–2530.

Cook, T.D., and D.T. Campbell. 1979. The design and conduct of quasi-experiments and true experiments in field settings. In *Handbook of industrial and organizational psychology*, ed. M.D. Dunnette, 223–326. Chicago: Rand McNally.

Crow, W., & Bull, J. (1975). Robbery deterrence: An applied behavioral science demonstration—final report. La Jolla: Western Behavioral Science Institute.

Crowe, T.D. 2000. *Crime prevention through environmental design: Applications of architectural design and space management concepts*. Oxford: Butterworth-Heinemann.

Cozens, P. 2008. Crime prevention through environmental design in Western Australia: Planning for sustainable urban futures. *International Journal of Sustainable Development and Planning* 3 (3): 272–292.

Cozens, P. 2016. *Think crime! Using evidence, theory and crime prevention through environmental design (CPTED) for planning safer cities*. Praxis education.

Cozens, P., and T. Love. 2015. A review and current status of crime prevention through environmental design (CPTED). *Journal of Planning Literature* 30 (4): 393–412.
Cozens, P.M., G. Saville, and D. Hillier. 2005. Crime prevention through environmental design (CPTED): A review and modern bibliography. *Property Management* 23 (5): 328–356.
Currie, E. 1993. *Reckoning: Drugs, the cities and the American future*. New York: Hill and Wang.
Department of Urban Affairs and Planning. 2001. Crime prevention and the assessment of development applica- tions: section 79c of the Environmental Planning and Assessment Act 1979. Retrieved May 7, 2020 from https://www.police.nsw.gov.au/data/assets/pdffile/0003/9390/duapguides79c.pdf.
Donner, C.M., C.D. Marcum, W.G. Jennings, G.E. Higgins, and J. Banfield. 2014. Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior* 34: 165–172.
Eck, J.E., and J. Wartell. 1996. Improving the management of rental properties with drug problems: A randomized experiment. *Crime Prevention Studies* 9: 161–185.
Ekblom, P. 2011. Deconstructing CPTED… and reconstructing it for practice, knowledge management and research. *European Journal on Criminal Policy and Research* 17 (1): 7–28.
Ekblom, P., R. Armitage, L. Monchuk, and B. Castell. 2013. Crime prevention through environmental design in the United Arab Emirates: A suitable case for reorientation? *Built Environment* 39 (1): 92–113.
Farrington, D.P., D.C. Gottfredson, L.W. Sherman, and B.C. Welsh. 2002. *The Maryland scientific methods scale. Evidence-based crime prevention*. New York: Routledge.
Farinholt, Brown, Mohammad Rezaeirad, Paul Pearce, Hitesh Dharmdasani, Haikuo Yin, Stevens Le Blond, Damon McCoy, and Kirill Levchenko. 2017. To catch a ratter: Monitoring the behavior of amateur darkcomet rat operators in the wild. In *2017 IEEE symposium on security and privacy (SP)*, pp. 770–787. IEEE.
Fisher, D.G., and A. Piracha. 2012. Crime prevention through environmental design: A case study of multi-agency collaboration in Sydney, Australia. *Australian Planner* 49 (1): 79–87.
Fisher, D.G., P. Wadds, and G. Clancey. 2018. The patchwork of alcohol-free zones and alcohol-prohibited areas in New South Wales (Australia). *Safer Communities* 17 (2): 94–102.
Geason, S., and P.R. Wilson. 1989. *Designing out crime: Crime prevention through environmental design*, vol. 3. Canberra: Australian Institute of Criminology.
Geers, K. 2010. The challenge of cyber attack deterrence. *Computer Law & Security Review* 26 (3): 298–303.
Gibson, V., and D. Johnson. 2016. CPTED, but not as we know it: Investigating the conflict of frameworks and terminology in crime prevention through environmental design. *Security Journal* 29 (2): 256–275.
Giles-Corti, B., A. Vernez-Moudon, R. Reis, G. Turrell, A.L. Dannenberg, H. Badland, S. Foster, M. Lowe, J.F. Sallis, M. Stevenson, and N. Owen. 2016. City planning and population health: A global challenge. *The Lancet* 388 (10062): 2912–2924.
Gotham, K.F., and D.B. Kennedy. 2019. Analyzing crime foreseeability: Premises security litigation and the case of convenience stores and gas stations. *Security Journal*. https://doi.org/10.1057/s41284-019-00218-1.
Grabosky, P.N. 2001. Virtual criminality: Old wine in new bottles? *Social & Legal Studies* 10 (2): 243–249.
Holt, Thomas J. 2017. On the value of honeypots to produce policy recommendations. *Criminology & Public Policy* 16 (3): 739–747.
Grabosky, P. 2016. The evolution of cybercrime, 2006–2016. In *Cybercrime through an interdisciplinary lens*, 29–50. London: Routledge.
Haider, M.A., and P. Iamtrakul. 2018. Theoretical concepts of crime and practices in urban planning and design process for safe urban life. *International Journal of Building, Urban, Interior and Landscape Technology* 12: 7–24.
Holt, T.J. 2007. Subcultural evolution? Examining the influence of on-and off-line experiences on deviant subcultures. *Deviant Behavior* 28 (2): 171–198.
Holt, T.J. 2017. On the value of honeypots to produce policy recommendations. *Criminology & Public Policy* 16 (3): 739–747.
Holt, T.J., and A.M. Bossler. 2013. Examining the relationship between routine activities and malware infection indicators. *Journal of Contemporary Criminal Justice* 29 (4): 420–436.

Holt, T.J., and A.M. Bossler. 2014. An assessment of the current state of cybercrime scholarship. *Deviant Behavior* 35 (1): 20–40.

Holt, T.J., A.M. Bossler, and D.C. May. 2012. Low self-control, deviant peer associations, and juvenile cyberdeviance. *American Journal of Criminal Justice* 37 (3): 378–395.

Holt, T.J., A.M. Bossler, and K.C. Seigfried-Spellar. 2018. The future of cybercrime, terror, and policy. In *Cybercrime and digital forensics: An introduction*, 623–652. London: Routledge.

Holtfreter, K., M.D. Reisig, and T.C. Pratt. 2008. Low self-control, routine activities, and fraud victimization. *Criminology* 46 (1): 189–220.

Huang, C., J. Han, X. Zhang, and J. Liu. 2019. Automatic identification of honeypot server using machine learning techniques. *Security and Communication Networks*. https://doi.org/10.1155/2019/2627608.

Jacobs, J. 1961. *The death and life of Great American Cities*. New York: Vintage.

Jeffery, C.R. 1977. *Crime prevention through environmental design*. Beverly Hills, CA: Sage.

Kaâniche, M., Deswarte, Y., Alata, E., Dacier, M., and Nicomette, V. 2006. Empirical analysis and statistical modeling of attack processes based on honeypots. In *IEEE/IFIP international conference on dependable systems and networks (DSN-2006), workshop on empirical evaluation of dependability and security (WEEDS)* (pp. 119–124). IEEE Computer Society.

Kigerl, A. 2016. Cyber crime nation typologies: K-Means clustering of countries based on cyber crime rates. *International Journal of Cyber Criminology* 10 (2): 147–169.

Kitchen, T., and R.H. Schneider. 2004. *Planning for crime prevention: A transatlantic perspective*. London: Routledge.

Kitchen, T., and R.H. Schneider. 2007. *Crime prevention and the built environment*. London: Routledge.

Lemos, Robert. 2013. Five reasons every company should have a honeypot. Dark Reading. Retrieved Oct 1, 2013 from darkreading.com/vulnerabilities—threats/5-reasons-everycompany-should-have-a-honeypot/d/d-id/1140595.

Leukfeldt, E.R., and M. Yar. 2016. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior* 37 (3): 263–280.

Lewis, J. 2018. *Economic impact of cybercrime: No slowing down report*. Santa Clara, CA: McAfee.

Maimon, D., M. Alper, B. Sobesto, and M. Cukier. 2014. Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology* 52 (1): 33–59.

Maimon, D., and E.R. Louderback. 2019. Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology* 2: 191–216.

McCamley, P. 2001. *Crime, design and urban planning: From theory to practice*. New Planner: Royal Australian Planning Institute.

McGuire, M. 2007. *Hypercrime: The new geometry of harm*. Cavendish: Routledge.

McQuade, S.C. 2006. *Understanding and managing cybercrime*. Boston: Pearson/Allyn and Bacon.

Minnery, J.R., and B. Lim. 2005. Measuring crime prevention through environmental design. *Journal of Architectural and Planning Research* 22 (4): 330–341.

Moffatt, R.E. 1983. Crime prevention through environmental design: A management perspective. *Canadian Journal of Criminology* 25 (1): 19–31.

Mohammadzadeh, H., Mansoori, M., and Welch, I. 2013. Evaluation of fingerprinting techniques and a windows-based dynamic honeypot. In *Proceedings of the eleventh Australasian information security conference-volume 138* (pp. 59–66). Australian Computer Society, Inc..

Nagin, D.S. 1998. Criminal deterrence research at the outset of the twenty-first century. *Crime and Justice* 23: 1–42.

Navarro, J.N., and J.L. Jasinski. 2013. Why girls? Using routine activities theory to predict cyberbullying experiences between girls and boys. *Women & Criminal Justice* 23 (4): 286–303.

Newman, O. 1972. *Defensible space*. New York: Macmillan.

Ngo, F.T., and R. Paternoster. 2011. Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology* 5 (1): 773–793.

Parnaby, P. 2006. Crime prevention through environmental design: Discourses of risk, social control, and a neo-liberal context. *Canadian Journal of Criminology and Criminal Justice* 48 (1): 1–30.

Peeters, M.P., and T.V. Beken. 2017. The relation of CPTED characteristics to the risk of residential burglary in and outside the city center of Ghent. *Applied Geography* 86: 9.

Pogarsky, G. 2002. Identifying "deterrable" offenders: Implications for research on deterrence. *Justice Quarterly* 19 (3): 431–452.

Reynald, D.M. 2011. Translating CPTED into crime preventive action: A critical examination of CPTED as a tool for active guardianship. *European Journal on Criminal Policy and Research* 17 (1): 69–81.

Ruiz-Sánchez, M.Á., E.W. Biersack, and W. Dabbous. 2001. Survey and taxonomy of IP address lookup algorithms. *IEEE Network* 15 (2): 8–23.

Sampson, R.J. 2010. Gold standard myths: Observations on the experimental turn in quantitative criminology. *Journal of Quantitative Criminology* 26 (4): 489–500.

Shah, R.C., and J.P. Kesan. 2007. How architecture regulates. *Journal of Architectural and Planning Research* 24: 350–359.

Sherman, L.W. 1990. Police crackdowns: Initial and residual deterrence. *Crime and Justice* 12: 1–48.

Sherman, L.W. 2007. The power few: Experimental criminology and the reduction of harm. *Journal of Experimental Criminology* 3 (4): 299–321.

Sherman, L.W., D.C. Gottfredson, D.L. MacKenzie, J. Eck, P. Reuter, and S. Bushway. 1997. *Preventing crime: What works, what doesn't, what's promising: A report to the United States Congress*. Washington, DC: US Department of Justice, Office of Justice Programs.

Sohn, D.W. 2016. Residential crimes and neighbourhood built environment: Assessing the effectiveness of crime prevention through environmental design (CPTED). *Cities* 52: 86–93.

Sorg, E.T., J.D. Wood, E.R. Groff, and J.H. Ratcliffe. 2017. Explaining dosage diffusion during hot spot patrols: An application of optimal foraging theory to police officer behavior. *Justice Quarterly* 34 (6): 1044–1068.

Spitzner, L. 2003. *Honeypots: Tracking hackers*. Reading: Addison-Wesley.

Steinmetz, K.F. 2015. Craft (y) nessAn ethnographic study of hacking. *The British Journal of Criminology* 55 (1): 125–145.

Stockman, M., R. Heile, and A. Rein. 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 (RIIT '15)*, 19–22. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2808062.2808069.

Stoll, C. 1989. *The cuckoo's egg: tracking a spy through the maze of computer espionage*. New York: Doubleday.

Sutton, A., A. Cherney, and R. White. 2008. *Crime prevention: principles, perspectives and practices*. Cambridge: Cambridge University Press.

Taylor, P. 1999. *Hackers: Crime and the digital sublime*. London: Routledge.

Taylor, R. 2002. Crime prevention through environmental design (CPTED): Yes, no, maybe, unknowable, and all of the above. In R. Bechtel & A. Churchman (Eds.), *Handbook of Environmental Psychology* (pp. 413–426).

Testa, A., D. Maimon, B. Sobesto, and M. Cukier. 2017. Illegal roaming and file manipulation on target computers: Assessing the effect of sanction threats on system trespassers' online behaviors. *Criminology & Public Policy* 16 (3): 689–726.

United Nations. 2007. Making cities safer from crime: The Safer Cities Programme, UN-Habitat. Activities Brief. http://www.unhabitat.org/safercities.

van den Bos, M., and L. Nell. 2006. Territorial bounds to virtual space: Transnational online and offline networks of Iranian and Turkish-Kurdish immigrants in the Netherlands. *Global Networks* 6 (2): 201–220.

Vagi, K.J., M.R. Stevens, T.R. Simon, K.C. Basile, S.P. Carter, and S.L. Carter. 2018. Crime Prevention Through Environmental Design (CPTED) characteristics associated with violence and safety in middle schools. *Journal of School Health* 88 (4): 296–305.

Waldrop, M.M. 2016. How to hack the hackers: The human side of cybercrime. *Nature News* 533 (7602): 164.

Weisburd, D., A. Petrosino, and G. Mason. 1993. Design sensitivity in criminal justice experiments. *Crime and justice* 17: 337–379.

Whitford, T. 2018. Cyber defense for IMGs and NGOs using crime prevention through environmental design. In *Cyber weaponry. Advanced sciences and technologies for security applications*, ed. H. Prunckun. New York: Springer.

Wilson, J.Q., and G.L. Kelling. 1982. Broken windows. *Atlantic Monthly* 249 (3): 29–38.

Wilson, T., D. Maimon, B. Sobesto, and M. Cukier. 2015. The effect of a surveillance banner in an attacked computer system: Additional evidence for the relevance of restrictive deterrence in cyberspace. *Journal of Research in Crime and Delinquency* 52 (6): 829–855.

Yar, M. 2005. Computer hacking: Just another case of juvenile delinquency? *The Howard Journal of Criminal Justice* 44 (4): 387–399.

Zahm, D. 2005. Learning, translating, and implementing CPTED. *Journal of Architectural and Planning Research* 22: 284–293.