British Journal of Criminology Advance Access published January 5, 2015

doi:10.1093/bjc/azu104 BRIT. J. CRIMINOL

ON THE RELEVANCE OF SPATIAL AND TEMPORAL DIMENSIONS IN ASSESSING COMPUTER SUSCEPTIBILITY TO SYSTEM TRESPASSING INCIDENTS

David Maimon*, Theodore Wilson, Wuling Ren and Tamar Berenblum

We employ knowledge regarding the early phases of system trespassing events and develop a context-related, theoretically driven study that explores computer networks' social vulnerabilities to remote system trespassing events. Drawing on the routine activities perspective, we raise hypotheses regarding the role of victim client computers in determining the geographical origins and temporal trends of (1) successful password cracking attempts and (2) system trespassing incidents. We test our hypotheses by analyzing data collected from large sets of target computers, built for the sole purpose of being attacked, that were deployed in two independent research sites (China and Israel). Our findings have significant implications for cyber-criminological theory and research.

Key words: system trespassing, routine activities, victims, target computer

Introduction

Computers and computer networks (i.e. interconnected collections of autonomous computers that allow an easy exchange of information between users, Tanenbaum 2003) have become such an integral part of industry, business and government that their smooth operation is increasingly critical to the survival of many European countries (Fritzon *et al.* 2007). Acknowledging the need for more secure computing environments, extensive technological research investigates the tools and methods employed by system trespassers (also known as hackers) in their attempts to infiltrate organizational computers (Allen and Stoner 2000; Mckey 2003). Nevertheless, only a few previous criminological initiatives have explored the way computer network users expose their client computers to system trespassing events (Demetriou and Silke 2003; Maimon *et al.* 2013). This is unfortunate because the frequency of system trespassing events in large organizations and the average cost of a single data breach for an organization ($5.4 million in 2012) have grown consistently (Ponemon Institute 2013).

We suspect that the underlying reason for the absence of criminological research on these vulnerabilities is embedded in criminologists' limited familiarity with system trespasser's online tactics, which feed on legitimate network users' online routines to gain illegal access to both computers and computer networks. Addressing this gap, this paper begins with a description of the different activities taken by system trespassers prior to the initiation of a system trespassing event that exploit legitimate users' activities on the network. Following that, we draw on the routine activities perspective (Hindelang *et al.* 1978; Cohen and Felson 1979) to formulate hypotheses regarding how

*David Maimon and Theodore Wilson, Department of Criminology and Criminal Justice, University of Maryland, 2220 LeFrak Hall, College Park, MD 20742; dmaimon@umd.edu; Wuling Ren, College of Computer and Information Engingeering, Zhejiang Gongshang University, Hangzhou, China; Tamar Berenblaum, Institute of Criminology, The Hebrew University, Jerusalem, Israel.

the daily online routines and physical geographical location of computer network users relate to the daily trends and geographical origins of (1) successful attempts by system trespassers to guess login passwords to victims computers (i.e. *brute-force attacks*), and (2) initial *system trespassing incidents* against computer networks' client computers. To test our hypotheses, we analyze unique data gathered by a large set of target computers built for the sole purpose of being attacked, which were deployed on the computer networks of a Chinese academic institution and an Israeli academic institution.

Theoretical Background

The anatomy of a system trespassing event

System trespassing (also known as hacking or cracking, Yar 2006) involves the unauthorized entry into a computer or computer network by someone who does not have legitimate access rights (Brenner 2010) and can occur either locally (when an illegitimate user has physical access to the target computer) or remotely (via the Internet, Stallings 2005; Engebretson 2013). The consequences of system trespassing depend on the system trespassers' motivation (e.g. monetary gain, intellectual challenge, revenge, industrial espionage), and may range from data and financial losses to emotional, psychological and physical harm to victims (McQuade 2006). Nevertheless, regardless of how and why trespassers access the target computers, they follow the same basic steps before they initiate a successful system trespassing incident. These steps inevitably feed on victims' uses of their computer networks.

Reconnaissance (also called profiling) is the first step taken by an intruder in preparation for system trespassing (Wilson 2001; Engebretson 2013). This process involves gathering public information on the would-be target-network from the Internet by posing as a regular user. In this stage, intruders gather intelligence on the organizational computer network and the information technology (IT) managers who maintain it, the machines and servers used by the organization and the individuals who are using the network computers (Hutchins *et al.* 2011). Large companies and organizations are likely to receive special attention from potential intruders due to the organizations' publicity efforts (through their websites and self-advertisements) and the independent attention they receive in the popular media.

The second phase in preparation for a system intrusion involves a *scan* of the organizational computer network. This more intrusive phase requires the use of port scanners to reveal active and available networked computer ports: ports configured to accept information from the network (Christopher 2001; Gadge and Patil 2008; Engebretson 2013).[1] The information collected by the scan allows offenders to map the networked computers' vulnerabilities (i.e. a weakness in software or hardware on a server or a client, Zago-Swart 2001; Kizza 2005), which could then be exploited.[2] Importantly, in many cases, computer users can fix these vulnerabilities but simply fail to do so. For instance, most new computer systems are sent to their new owners with a default configuration and known inherent vulnerabilities, which allow intruders easy access to the

[1] Port scanners like Nmap are available to download from the Internet for free.

[2] Even though potential intruders look for vulnerabilities on the network by checking 'which door is unlocked', an intrusion has yet to occur and no laws have been broken at this stage.

system. Changing the default configurations of the system to a customized configuration eliminates this issue. Similarly, installing readily available software updates periodically may prevent intrusion into the system.

In the third step taken by potential intruders before launching a system trespassing event, offenders gather intelligence on the network users' accounts and attempt to obtain the correct passwords to these accounts (Boyd 2000; Long 2008). Potential intruders employ two major tactics in efforts to obtain their goals in this *enumeration* phase. Employing the first tactic, known as *phishing,* potential intruders identify legitimate users of the network (usually via email) and use a range of social engineering tactics (threatening, lying, asserting authority, etc.) to convince their targets to provide their usernames and passwords or to download malware (i.e. viruses, worms or Trojans) to their computers (Long 2008).[3] The second approach for obtaining network users' passwords involves the use of special software (for instance, Wireshark and Cain) that monitors the incoming and outgoing traffic to/from the target computer. Eavesdropping on networked computers allows potential intruders to learn about the computer network users' online routines (for instance, which websites they are more likely to browse, how often and when they use the network, etc.) as well as look for users' passwords (Cheng *et al.* 2013). Importantly, would-be-targets' awareness of these enumeration tactics attenuate potential intruders' success rates in obtaining valuable information (McQuade 2006; Long 2008).

The fourth stage involves the *exploitation* of vulnerabilities and an actual attempt to infiltrate the system (Erickson 2008; Hutchins *et al.* 2011). In this phase, system trespassers use various attacking tools that take advantage of computer vulnerabilities identified in the preceding phases (Wilson 2001; Garfinkel *et al.* 2003: xxiv). For instance, using the information obtained in the scanning stage about software used by legitimate users, trespassers may seek software bugs that open holes in the system. At the same time, intruders will attempt to guess computer users' passwords to the target computers through the use of special 'brute-force' toolkits.[4] Shorter and simpler passwords can be cracked quickly, whereas longer passwords, especially those combining letters and numbers, serve as a more effective barrier to 'brute-force' toolkits.

The fifth and final phase in the anatomy of a system trespassing incident is the *initiation of a trespassing event.* In this phase, the intruder has successfully infiltrated the system and is now ready to work with it.[5] During the first trespassing incident, an intruder may attempt to conceal evidence of the intrusion and make sure he can easily return into the system at a later time by downloading software, installing a 'backdoor', or creating his own username and password on the system (Maimon *et al.* 2014). At this point, legitimate computer users can do little to prevent the trespassing event from progressing—in fact, in many cases, legitimate users are not even aware of the presence of a system trespasser on their computer. Nevertheless, understanding the preparatory phases of a first system trespassing incident is vital for conceptualizing and theorizing

[3] In effort to victimize as many computer users as possible, potential intruders also attempt to lure smartphone users to download malware on their devices by sending text messages and asking users to access fake websites. This modern form of phishing is called 'smishing' (a combination of SMS texting and phishing, Mu *et al.* 2013).

[4] A 'brute-force' toolkit is an automatic tool that tries combinations of characters in an attempt to discover a legitimate user's password to a system (Engebretson 2013).

[5] Importantly, some of the brute-force tools do not allow a clear distinction between the exploitation and initiation phases: some tools automatically initiate trespassing events once they crack legitimate usernames and passwords.

the role played by legitimate computer network users' online routines (Wilson 2001) in exposing their computers and networks to system trespassing events.

The routine activities/lifestyle perspectives

The routine activities and lifestyle perspectives are the most prominent models utilized by modern criminologists for explaining legitimate computer users' online routines and susceptibility to cybercrime (Marcum *et al.* 2010; Reyns *et al.* 2011). Overall, the classical routine activities theory strives to single out behaviours, activities and situational contexts that put would-be targets at higher risk for criminal victimizations (Cohen and Felson 1979). In their early elaboration of the theory, Cohen and Felson proposed that the structure of collective daily routines dictates the convergence in time and space of motivated offenders, suitable targets and available guardians, and influences trends of predatory crime (i.e. criminal events in which an offender purposefully takes or damages another person or another person's property, Glaser 1971: 4). Pinpointing the role of criminal opportunities in their perspective, Cohen and Felson (1979) attributed the sharp rise in the US crime rates between the 1950s and 1970s to the diffusion of routine activities away from the American household. Moreover, these scholars claimed that certain technological developments (for instance, changes in the size and weight of consumer durables) altered the nature of criminal victimization and determined potential targets' chances of becoming victims of crime (Cohen 1981).

Likewise, Hindelang and associates (1978) argued that individuals are more likely to become victims of crime the more often they come in contact with members of groups that include a disproportionate share of offenders. Specifically, these scholars suggested that varying levels of exposure to motivated offenders is a function of would-be targets' socio-demographic characteristics (e.g. age, sex, race and marital status) and lifestyles (Sampson and Lauritsen 1990). An individual's socio-demographic characteristics form the core of his or her daily routines, and in turn, determine exposure to capable offenders and the risk of criminal victimization (Sampson and Lauritsen 1990). Due to the shared theoretical assumptions of the routine activities and lifestyle theories, the two models are considered complementary and establish a unique and distinct theoretical perspective (Reyns *et al.* 2011).

In an effort to evaluate the theoretical claims promoted by the routine activities and lifestyle perspectives, extensive research initiatives have been launched in both the United States and abroad (Messner and Blau 1987; Fischer *et al.* 1998; Vazsonyi *et al.* 2002). These studies have found support for the premise that exposure to motivated offenders during daily routines inflates the likelihood of criminal victimization. Moreover, an extensive body of research indicates that geographical proximity to motivated offenders increases the likelihood that would-be targets experience property crimes (Brantingham and Brantingham 1991 1995; Wright and Decker 1994) and violent crimes (Canter and Larkin 1993; Alston 1994; Rossmo 1994; Johnson and Bowers 2007).

Recently, several scholars have applied the routine activities perspective to the study of cybercrime (Holt and Bossler 2009; Pratt *et al.* 2010). Most of these studies report that computer users' daily online routines (for instance, Internet website purchasing and chat room participation) increase users' risks of online fraud (Pratt *et al.* 2010),

cyber-harassment (Holt and Bossler 2009) and malware victimization (Bossler and Holt 2011). Although their results generally support the application of routine activities theory in the context of cyberspace, a few theoreticians have raised concerns regarding the applicability of the model in cyberspace. Specifically, Yar (2005) contends that utilizing the routine activities theory in the context of cyberspace is debatable, as it is difficult to posit that convergence in space and time is analogous between cybercrimes and more traditional crimes. Concerning the *spatial dimension* of cyberspace, Yar (2005) acknowledges that the efficiency of Internet communication depends on the physical location of both the data and the Internet hardware through which the data traverse (for instance, routers, fibre optics cables, phone lines, etc.), as well as the actual distance through which communication between two computers travels (Goldsmith and Wu 2006; Dodge and Zook 2009). Nevertheless, Yar (2005) believes that as the average lifespan of virtual places (for instance, webpages) is relatively short (a couple of months), these virtual locations refute Cohen and Felson's (1979) premise that places have a stable and fixed presence, and complicate the adoption of the theory in the context of cyberspace. Although Yar's (2005) claim could be relevant for Internet websites, it may not be valid when applied to computer networks employed by large organizations. Specifically, universities, governmental agencies and commercial organizations rely heavily on their computer networks to ensure the smooth functioning of their services, as well as to store users' personal information and records (McQuade 2006). Both employees and customers routinely use these computer networks, and their presence in the cyber environment is fairly stable.

Speculating on the *temporal dimension* of cyberspace, Yar (2005) further asserts that the temporal convergence of cyber-victims, cyber-offenders and cyber-guardians is problematic because the cyber world is populated continuously and thus there are no particular times at which actors are expected to be either present or absent from the environment. Although Yar's claim is appreciated, it may not be applicable in the context of computer networks and its users. Specifically, as some computer networks are more active during specific times of the day (universities and schools), week (commercial entities), month (small business billing cycles) or year (National Science Foundation, a funding agency in the United States, and Institutional Revenue Service, the tax collection agency in the United States), they may face a similar temporal victimization risk as in traditional crimes like robbery and burglary. A recent study by Maimon and colleagues' (2013) confirms this observation. Thus, in line with past research, we view the routine activities perspective (Cohen and Felson 1979) as an adequate framework for understanding the role of system trespassing victims in exposing their computer networks to system trespassers' attempts to guess victims' computer passwords and initiate system trespassing events against the system.

The present study

Drawing on the routine activities perspective, our study focuses on the last two phases in the anatomy of a system trespassing event: exploitation and trespassing. Specifically, we seek to explore the relationships between a computer network's geographical location, its users' daily online routines, and the geographical origin and timing of (1) successful attempts by system trespassers to guess login passwords to victims' computers (hereafter, brute-force attacks) and (2) system trespassing events against computer

networks' client computers. By focusing on exploitation and trespassing, we join prior criminologists (Sullivan 1989; Wright and Decker 1994; Brantingham and Brantingham 1995; Johnson and Bowers 2007) and advance a context-embedded approach for the study of criminals' and victims' behaviours during different phases of a criminal event. This approach allows us to form more refined, educated and context-related hypotheses regarding the varying levels of a victim's responsibility during different phases of a trespassing incident.

Considering first the geographical origin of successful brute-force attacks against computer networks' client computers, we adopt Brantingham and Brantingham's (1995) view that victimization patterns are tied to the victims' routine paths (i.e. where people go) and suspect that computer networks' geographic locations determine the geographical origin of successful brute-force attacks against the network client computers. Indeed, cyberspace is considered by many to be a homogenous place, in which any individual from any locale is just a click away. However, in reality, cyberspace is composed of numerous physical and regional networks (known as autonomous systems), which are responsible for choosing the peer networks they will interchange data with and route Internet traffic through (Tanenbaum 2003). As a consequence, more Internet traffic (i.e. connections between users and webpages, sending and receiving emails, etc.) is increasingly concentrated within localities, countries and regions (Murnion and Healy 1998; Thelwall 2002), and declines with distance. Related to this, Goldsmith and Wu (2006) observe that users around the globe experience the Internet differently, in ways that correspond to geographical boundaries. Adopting the premise that nearby residents tend to have a lot in common compared with people on the other side of the world, these scholars suggest that language, culture, currency and consumer norms translate into different inclinations and desires among Internet users, and result in online routines and behaviours that coincide with geographical places and regions. Thus, *we propose that computer network users are more likely to expose their networks to regional malicious Internet traffic and automated tools, and experience a high volume of successful brute-force attacks from nearby geographical regions of the world.*

Consistent with the view that geographical distance in cyberspace determines the Internet performance, we also believe that initial system trespassing incidents on attacked networked computers are likely to originate from geographical regions of the world that are proximate to the physical location of the attacked computer network. Overall, the time that it takes to transport and receive data between two nodes on the Internet depends on the length of the line connecting those two nodes.[6] Therefore, in an effort to improve the service to their customers and speed up communication between servers and clients, companies like Cisco and others ask their users to choose a nearby server before downloading a file to their computers (Goldsmith and Wu 2006). Similarly, we suspect that the physical location of the attacked computer system determines the geographical location through which a first system trespassing incident is initiated against it. Importantly, our research focuses on the *geographical location of the attacking computers* and not on the geographical location of the system trespasser. For instance, it is possible that a system trespasser who sits behind a computer in the United

[6] Routing time also depends on the quality of the line, the quality of the intermediate servers, the quality of the two hosts and the current usage of the line.

States will utilize a computer in India to initiate a first system trespassing event on a target computer located in China (Long 2008). However, in line with the idea that offenders' cognitive maps allow them to identify places with good opportunities to offend (Johnson and Bowers 2007), we believe that in order to improve connectivity and speed to the target computers, system trespassers choose to initiate first trespassing incidents from computers located geographically proximately to the victim's target computer. Specifically, as system trespassers tend to download software and other files to the attacked computers, we suspect *that first system trespassing incidents originate in proximate geographical regions to the attacked computer system.*

Alongside the spatial dimension of successful password-guessing attempts and system trespassing incidents, we also speculate on the time of day during which these events occur. Indeed, prior research has already indicated that the daily online routines of computer network users determine the timing of computer-focused crimes (e.g. DoS attacks, exploits and port scans) against a computer network (Maimon *et al.* 2013). However, although Maimon and colleagues focus on DoS attacks and the early stages of system trespassing incidents in their work (i.e. scanning and enumeration), our study explores more advanced stages of a trespassing event (i.e. exploitation and system trespassing). Nevertheless, we adopt Maimon *et al.*'s (2013) rationale and suspect that *as many network users (employees and clients) are likely to use the network during the official network activity times, networked computers are likely to experience a high volume of successful brute-force attacks during that time.*

Finally, in contrast to the expected daily trend of successful brute-force attacks against network computers, we believe that routine activities theory is less effective for predicting daily trends of first system trespassing incidents (Bossler and Holt 2009). Specifically, unlike password-guessing attempts that depend on the victims' daily routines and require the target computers to stay online for prolonged periods of time (in order for the brute-force tool to 'guess' the correct password), system trespassing incidents are mostly dependent on trespassers' decisions of when to initiate the trespassing event. Thus, since once a system trespasser has obtained the credentials to a target computer he/she can initiate a system trespassing event at any time he/she chooses, *we expect that first system trespassing incidents will not follow any specific daily trend.*

Data and Methods

To test our research hypotheses and at the same time preserve the unique context in which remote password-guessing attempts and system trespassing incidents occur, we collected data directly from the Internet. Our data collection procedure involved using a series of target computers called 'Honeypots'.

Data collection

A Honeypot is a 'security resource whose value lies in being probed, attacked or compromised' (Spitzner 2002: 40). This technological tool is a real computer that enables the collection of information on real-system trespassing incidents. As Honeypots have no production value, any network activity that is sent their way means that system trespassers are looking to infiltrate the system, compromise it and employ it for their malicious operations. Although IT teams employ production Honeypots to detect

and mitigate attacks against their networks, cybersecurity scholars deploy research Honeypots to explore who the attackers are, what they are doing on the compromised systems and what kind of tools they use (Spitzner 2002). Consistent with past criminological (Maimon *et al.* 2014) and technological studies (Salles-Loustau *et al.* 2011), we deployed research Honeypots (which will be identified as target computers henceforth) on the computer networks of two Chinese and Israeli academic institutions, and collected information on successful brute-force attacks and system trespassing incidents against the target computers on these networks.

At the Chinese research site, we utilized 240 public IP addresses[7] that were provided to us by the IT team of a large Chinese university, and deployed our target computers on the university network. These target computers were set up as computer systems with the Linux Ubuntu 10.04 operating system. We deployed our target computers on the University network for a period of four months (21 August 2012–21 December 2012), and waited for system trespassers to find our systems and employ special software cracking tools to successfully guess the 'correct' password into them. We created a genuine computer network environment by programming the target computers to deny intruders' login attempts on public IP addresses until a predefined threshold was reached. This predefined threshold was a random number between 150 and 200. When this threshold was reached, the target computer was 'successfully' infiltrated and allowed intruders to initiate a system trespassing incident. Following infiltration, we allowed system trespassers to employ the target computers for a period of 30 days. At the end of the 30-day period, we blocked the system-trespasser's access to the target computer, cleaned the system and redeployed it on the network.

Our research team at the Israeli site employed a similar research design. However, only 60 public IP addresses were employed for the deployment of target computers on the Israeli network. Moreover, data collection efforts took place over a three-month period (23 May 2013–31 August 2013). Although the different number of IP addresses available at the Israeli and Chinese research sites contributes directly to the respective numbers of incidents recorded against the target computers, we have no reason to believe that it could bias the temporal trends and geographical origin of brute-force attacks and trespassing incidents against the networks' computers.

Outcome measures

In line with prior conceptualizations of password-guessing attempts (Keith *et al.* 2005; SANS Institute 2007), we operationalize a successful brute-force attack as any event in which an unauthorized person or automatic tool successfully guesses the password to a system. Thus, we consider any target computer that was subject to a successful remote password-guessing attempt a victim of a brute-force attack. Similarly, we follow prior conceptualizations of system trespassing incidents (Berthier and Cukier 2009; Maimon *et al.* 2014) and operationalize a first system trespassing event as any incident in which an unauthorized person accesses and logs in to a computer system for the first time.

[7] An IP address is an identifier for a computer or device on the network. There are two formats of IP addresses currently employed—IPv4 and IPv6. The format of an IPv4 address (those used in the current study) is a 32-bit numeric address written as four numbers separated by periods (e.g. 12.163.10.234). In most cases, Internet Service Providers assign IP addresses to their clients for a limited time period. These IP addresses are associated with specific countries and geographical regions of the world.

Consequently, any target computer that was subject to an actual system trespassing event is considered a victim of 'system-trespassing' in our sample.[8]

Overall, a total of 752 Chinese target computers experienced brute-force attacks throughout the data collection period. These attacks originated in 347 unique IP addresses. However, not all system trespassers initiated a system trespassing incident against our target computers: only 301 Chinese target computers recorded a first system trespassing incident (these incidents were initiated from 140 unique IP addresses). In contrast, due to the low number of IP addresses employed at the Israeli site, only 118 Israeli target computers experienced brute-force attacks during the data collection period. These attacks originated in 115 unique IP addresses. Similarly, first system trespassing incidents were initiated from 60 unique IP addresses against our 72 Israeli computers.

Independent measures

To identify the geographical origin from which brute-force attacks and system trespassing incidents were launched, we looked at the IP addresses used by system trespassers to access our target computers and classified them according to geographical regions of the world.[9] Importantly, as we did not have a way to collect the IP addresses of deviant computers that launched an 'unsuccessful' brute-force attack against our systems, we can only identify the geographical origin of 'successful' brute-force attacks and trespassing incidents. Moreover, the IP addresses available to us correspond to the last IP addresses used by system trespassers when initiating brute-force attacks and trespassing incidents against our systems. Consequently, these IP addresses coincide with the last geographical locations from which these incidents were launched (and not to the actual geographical location from which the intrusion originates) and are useful for determining whether trespassers attack from computers located in geographical proximity to the target computer.

Next to recording the spatial origin of the IP addresses observed on our target computers, we also observed the time in which each illegal event occurred. Specifically, we analyzed the time stamps of successful brute-force attacks and system trespassing incidents, and assigning them to three equal 8-hour intervals: 9 am–4:59 pm, 5 pm–12:59 am and 1 am–8:59 am.

Results

Geographical origin of successful brute-force attacks and first trespassing incidents

We begin by testing whether the geographical location of computer networks determines the region of the world through which the network clients' computers will be

[8] Indeed, as system trespassers were allowed to use the target computers for a period of 30 days, our target computers were the subjects of repeated system trespassing incidents. Nevertheless, analysis of the spatial distribution and timing of repeated system trespassing events is beyond the scope of our work because such analysis requires more extensive knowledge regarding the system trespassers, their motivation, resources and technical skills. As our focus in this work is on the victimized computers, we limit the scope of our analyses to successful brute-force attacks and first system trespassing incidents against the target computers.

[9] As some of the attacking IP addresses are responsible for more than one attack against our Chinese and Israeli computers, some may argue that the geographical distribution of brute-force attacks and trespassing events could be somewhat inflated when analyzing the entire list of attacking IP addresses. In analyses not shown, we rerun our analyses, while limiting our sample to attacks originated in unique IP address. Results from these analyses (available from the authors upon request) are identical to those reported in the text. We opt to present results from our analysis of the full sample of IP addresses because duplicating IP addresses do not necessarily mean that the same computer/user employed the IP address to generate an attack on our system.

accessed by system trespassers in attempts to guess their passwords. Applying our first hypothesis in the context of our research design, we believe that the majority of the Chinese target computers will experience brute-force attacks (i.e. remote password-guessing attempts) from IP addresses that originate in Asia. In contrast, we suspect that the majority of the Israeli target computers will experience brute-force attacks from IP addresses that originate in Europe. Table 1, Panel A, presents the origins of brute-force attacks on the Chinese and Israeli target computers.

Focusing first on the Chinese research site, we present on the far left side of Panel A the distribution of all target computers experiencing brute-force attacks ($N = 752$) from different geographical regions of the world. As may be noted in the table, the majority (68 per cent) of the Chinese target computers received brute-force attacks from IP addresses originated in Asia. Forty-one per cent of these IP addresses originated in China (334 computers). In contrast, only 14.7 per cent and 10 per cent, respectively, of the computers experienced brute-force attacks from computers originating in European and North American countries. To test whether these differences are significant, we employed a chi-squared test for goodness of fit (Snedecor and Cochran 1989) and compared the observed and expected counts of Chinese target computers that experienced brute-force attacks from different geographical regions of the world. Our statistical null hypothesis suggested that the proportions of target computers that experienced brute-force attacks from different geographical regions would be equal (i.e. 20 per cent of the target computers were brute forced from Europe, 20 per cent of the

TABLE 1 *Geographical origin of successful brute-force attacks and first system trespassing incidents against Chinese and Israeli target computers*

	Chinese site		Israeli site	
Panel A: Successful brute-force attacks, by region				
Region of the world	Target computers experiencing successful brute-force attacks($N = 752$), %	Target computers experiencing attacks originating at non-Chinese IP addresses ($N = 418$), %	Target computers experiencing successful brute-force attacks ($N = 118$), %	Target computers experiencing attacks originating at non-Chinese IP addresses($N = 77$), %
Europe	14.7	26.0	20.5	32.0
Asia	68.0	41.0	42.7	10.0
North America	9.3	16.7	19.0	30.0
South America	6.2	11.2	16.2	25.0
Middle East	1.0	2.0	–	–
Panel B: First system trespassing incidents, by region				
	Target computers experiencing first system trespassing events ($N = 301$), %	Target computers experiencing trespassing events originating at non-Chinese IP addresses ($N = 205$), %	Target computers experiencing first system trespassing events ($N = 72$), %	Target computers experiencing trespassing events originating at non-Chinese IP addresses ($N = 50$), %
Europe	23.6	34.0	33.3	50.0
Asia	64.1	47.0	41.7	14.0
North America	6.0	8.7	12.5	18.7
South America	5.6	8.3	9.7	14.5
Middle East	–	–	1.4	2.0

computers were brute forced from Asia, etc.). The alternative hypothesis was that the observed proportions of target computers experiencing brute-force attacks from different geographical regions would be different from the expected values. The estimated chi-square scores and p values indicated a statistically significant difference ($p < 0.01$) between the observed and expected frequencies of target computers that experienced brute-force attacks from different geographic regions of the world.

In order to test the robustness of this finding, we also examined the proportion of Chinese target computers that were brute force attacked from different geographical regions of the world, while excluding all computers that were accessed from Chinese IP addresses ($N = 418$ computers). Specifically, we suspect that as a large proportion of successful brute-force attacks originated in China, results from our analysis might be biased by this extreme value. As indicated in the second column of Panel A, excluding target computers that were brute force attacked by Chinese IP addresses from our analysis did not substantively change the geographical distribution of successful brute-force attacks against the Chinese target computers. Specifically, more than 40 per cent of the Chinese target computers were still attacked from Asian IP addresses, and only 16.7 per cent of the Chinese target computers were attacked by North American IP addresses. To test whether these differences are statistically significant, we reran a chi-square test for goodness of fit. The estimated chi-square scores and p values indicated a statistically significant ($p < 0.01$) difference between the observed and expected frequencies of Chinese target computers that received brute-force attacks from different geographic regions of the world.

We further explored our first research hypothesis with the Israeli data and present on the right side of Table 1, Panel A the distribution of all Israeli target computers that were subject to successful brute-force attacks ($N = 118$). At first glance, it looks like we find no support for this research hypothesis in the Israeli context. Specifically, when exploring the proportion of Israeli target computers that were brute force attacked from different geographical regions of the world, it seems that the majority of the target computers were attacked by Asian IP addresses (42.7 per cent) and that merely 20 per cent of the computers were attacked by European IP addresses. A closer look at the Asian IP addresses reveals that more than 31 per cent of the target computers were attacked by Chinese IP addresses. Therefore, we excluded these target computers from the analysis and re-examined the proportion of the target computers in Israel that were brute force attacked from different geographical regions of the world. Results from this analysis suggest that the majority of the Israeli target computers received successful brute-force attacks from European and North American IP addresses. However, the estimated chi-square test scores and p values associated with this finding indicate a statistically insignificant difference between the observed and expected frequencies of Israeli target computers that received successful brute-force attacks from different regions of the world.

Moving to our second research hypothesis, we explore whether *first system trespassing incidents* are likely to originate in geographical regions of the world that are proximate to the physical location of the attacked computer network. Results from this analysis are presented in Table 1, Panel B. Consistent with the finding reported for successful brute-force attacks, our findings indicate that the majority of Chinese target computers were infiltrated via IP addresses that originated in Asian countries, and that less than 10 per cent of the computers were infiltrated via North American IP addresses. The estimated chi-square scores and p values associated with this finding indicated a statistically

significant difference ($p < 0.01$) between the observed and expected frequencies of target computers infiltrated from different regions of the world, both when including ($N = 301$) and excluding ($N = 205$) target computers that were infiltrated via Chinese IP addresses. In line with the pattern reported for successful brute-force attacks on the Israeli computers, we also find that although it appears that the majority of the Israeli target computers were infiltrated via IP addresses originating in Asia, China is responsible for more than 30 per cent of the overall trespassing incidents recorded on the target computers. After omitting attacks originating at Chinese IP addresses from our analysis, we find that 50 per cent of the target computers experienced a first system trespassing incident via IP addresses originating in European countries. In contrast, only 14 per cent of the target computers were infiltrated from Asian countries outside China. Results from a chi-square test for goodness of fit further indicated a statistically significant difference ($p < 0.01$) between the observed and expected frequencies of Israeli target computers infiltrated from different regions of the world.

Timing of successful brute-force attacks and first trespassing incidents

Next, we explore the hypothesis that networked computers are likely to experience a high volume of successful brute-force attacks during the organization's normal business hours. As our target computers are deployed on the computer networks of two universities, we suspect that the majority of successful brute-force attacks will occur between 9 am and 5 pm, the official business hours for the two universities. Panel A in Table 2 presents the proportion of target computers that experienced successful brute-force attacks throughout the three equal time intervals.

Beginning with the trends observed on the Chinese research site, one may observe in the left side of Table 2, Panel A that the majority of the target computers experienced a successful password-guessing attempt between 9 am and 4:59 pm. Specifically, analysis of the timing of successful brute-force attacks recorded against our Chinese target computers ($N = 752$) indicates that more than 36 per cent of the target computers experienced successful brute-force attacks during university business hours. Nevertheless, the proportions of target computers that experienced successful brute-force attacks during the two other time intervals appear relatively equivalent. Thus, we utilized a chi-square test for goodness of fit and compared the observed and expected counts of target computers that experienced successful brute-force attacks in the three time intervals.

Our statistical null hypotheses suggested that the volume of target computers that experienced successful brute-force attacks in each eight-hour interval are equal (i.e. 33.3 per cent of the computers experienced brute-force attacks between 9 am and 4:59 pm, 33.3 per cent experienced attacks between 5 pm and 12:59 pm and 33.3 per cent experienced brute-force attacks between 1 am and 8:59 am), whereas the alternative hypothesis was that the observed frequencies are different from the expected frequencies. The estimated chi-square scores and p values indicated a statistically insignificant difference between the observed and expected frequencies for the Chinese target computers across the three time intervals. As a decent proportion of brute-force attacks originated at Chinese IP addresses, we test the robustness of this finding and traced the timing of attacks that originated at Chinese IP addresses ($N = 334$) and non-Chinese IP addresses ($N = 418$). As may be noted in the table, the majority of the Chinese

TABLE 2 *Temporal trends of successful brute-force attacks and first system trespassing incidents against Chinese and Israeli target computers*

	Chinese site			Israeli site		
Panel A: Successful brute-force attacks, by time of day						
Time of day	Target computers experiencing successful brute-force attacks (N = 752), %	Target computers experiencing attacks originating at Chinese IP addresses (N = 334), %	Target computers experiencing attacks originating at non-Chinese IP addresses (N = 418), %	Target computers experiencing successful brute-force attacks (N = 118), %	Target computers experiencing attacks originating at Chinese IP addresses (N = 41), %	Target computers experiencing attacks originating at non-Chinese IP addresses (N = 77), %
9 am–4:59 pm	36.3	38.3	35.0	53.4	53.6	53.2
5 pm–12:59 am	32.0	30.8	33.0	29.7	34.0	27.3
1 am–8:59 am	31.6	30.8	32.0	16.9	12.2	19.5
Panel B: First system trespassing incidents, by time of day						
	Target computers experiencing first system trespassing incidents (N = 301), %	Target computers experiencing trespassing incidents originating at Chinese IP addresses (N = 96), %	Target computers experiencing trespassing incidents originating at non-Chinese IP addresses (N = 205), %	Target computers experiencing first system trespassing incidents (N = 72), %	Target computers experiencing trespassing incidents originating at Chinese IP addresses (N = 22), %	Target computers experiencing trespassing incidents originating at non-Chinese IP addresses (N = 50), %
9 am–4:59 pm	38.9	23.0	46.3	43.0	27.3	50.0
5 pm–12:59 am	28.6	25.0	30.2	30.6	59.1	18.0
1 am–8:59 am	32.5	52.0	23.4	26.4	13.6	32.0

target computers experienced successful brute-force attacks from both Chinese (more than 38 per cent of incidents) and non-Chinese (more than 35 per cent) IP addresses between 9 am and 4:59 pm. Nevertheless, the estimated chi-square for the goodness of fit scores still indicated a statistically insignificant difference between our observed and expected frequencies of target computers throughout the three time intervals.

Turning to the Israeli research site, we present the proportion of target computers that experienced successful brute-force attacks during each time interval on the right side of Table 2, Panel A. Consistent with the findings reported for the Chinese target computers, the majority (more than 53 per cent) of Israeli target computers experienced successful brute-force attacks between 9 am and 4:59 pm. However, only a low number of Israeli target computers experienced successful brute-force attacks between 1 am and 8:59 am (almost 17 per cent of the target computers). The estimated chi-square scores and p values from the chi-square test for goodness of fit indicated a statistically significant difference ($p < 0.01$) between the observed and expected frequencies of these attacks.

As a substantial proportion of the successful brute-force attacks originated in China, we next trace the timing of successful brute-force attacks that originated at Chinese IP addresses (N = 41) and non-Chinese (N = 77) IP addresses. As may be noted in the table, the majority of successful brute-force attacks on Israeli target computers that

originated either at Chinese or non-Chinese IP addresses occurred between 9 am and 4:59 pm. In turn, only a small proportion of target computers experienced a successful brute-force attack between 1 am and 8:59 am. The estimated chi-square for goodness of fit scores indicated a statistically significant difference ($p < 0.01$) between the observed and expected frequencies of attacks from Chinese and non-Chinese IP addresses during the three time intervals.

Finally, we test our last research hypothesis, which suggests that first system trespassing incidents should not follow any specific daily trend. Panel B in Table 2 presents the proportion of target computers experiencing system trespassing incidents over the three time intervals. As indicated in the table, in contrast to the consistent daily trend observed for brute-force attacks against the Chinese and Israeli target computers, no similar trend is observed for first system trespassing incidents. Indeed, analyses of the entire pool of first system trespassing incidents recorded on our Chinese and Israeli target computers suggest that the majority of target computers experienced first system trespassing incidents during the two universities' respective business hours. Nevertheless, observing the daily trends of first system trespassing by Chinese and non-Chinese IP addresses suggests a different story. Although first system trespassing events originating at Chinese IP addresses and recorded on our Chinese computers are more frequent between 1 am and 8:59 am, first system trespassing events originating at Chinese IP addresses and recorded on our Israeli computers are more prevalent between 5 pm and 12:59 am. Similarly, although first system trespassing events originating at non-Chinese IP addresses and recorded on our Chinese computers are least frequent between 1 am and 8:59 am, first system trespassing events originating at non-Chinese IP addresses and recorded on our Israeli computers are more prevalent between 5 pm and 12:59 am.

Discussion

Although past research has focused on understanding system trespassers' tools and methods of operation, only a few previous studies have identified unique characteristics of computer networks that expose their client computers and users to system trespassing events (Demetriou and Silke 2003; Maimon *et al.* 2013). Addressing this challenge, we employed the routine activities perspective (Hindelang *et al.* 1978; Cohen and Felson 1979) to raise context-related hypotheses regarding the relationships between the geographical location and daily online routines of computer network users, and the geographical origin and daily trend of system trespassers' successful attempts to guess victims passwords (*brute-force attacks)* and to *initiate system trespassing incidents* against university networks' client computers. We first hypothesized that computer networks' geographic locations determine the geographical origin of successful brute-force attacks and first system trespassing incidents against client computers (Brantingham and Brantingham 1995). We also speculated that although networked computers are more likely to experience a high volume of successful brute-force attacks during the organization's business hours (Maimon *et al.* 2013), the timing of first system trespassing incidents should not coincide with legitimate network users' online routines. To test our hypotheses, we deployed two large sets of target computers—one set in China and one in Israel—built for the sole purpose of being attacked, and collected data on the

brute-force attacks and system trespassing incidents that were launched against these computers. Findings from our analyses revealed several important insights.

First, we find mixed evidence for the idea that computer networks' geographic locations determine the geographical origin of successful brute-force attacks. Specifically, our analysis indicates that the majority of successful brute-force attacks observed on the Chinese target computers originated at Asian IP addresses. Nevertheless, a less obvious pattern was reported in the Israeli site: there, the majority of brute-force attacks originated in Asian countries (42.7 per cent). It is only after omitting the attacks originating at Chinese IP addresses from the analysis (i.e. outliers) that we find that most of the successful brute-force attacks arrived from European and North American IP addresses. Aside from providing mixed support for our assumption that computer network users expose their networked computers to local malicious traffic and tools, as their Internet traffic is likely to be routed through local Internet hubs and as they share interest with nearby regional residents, these findings also demonstrate the extensive offensive efforts taken by Chinese hackers against a wide range of computer targets around the world (Ball 2011).

Stronger evidence for the importance of geographical proximity in cyberspace is revealed when we examine the geographical origin of first system trespassing incidents. Indeed, our findings indicate that the majority of first system trespassing incidents against the Chinese computers were initiated from Asian IP addresses, and that less than 10 per cent of the incidents originated at North American IP addresses. Moreover, we find that the majority of incidents recorded against the Israeli computers from non-Chinese IP addresses originated in European countries. These findings confirm Dodge and Kitchin's (2000) view that cyberspace does not consist of one homogenous space and join prior technical research suggesting that most of the Internet traffic becomes increasingly concentrated within localities, countries and regions (Murnion and Healy 1998; Thelwall 2002). Moreover, these findings extend Brantingham and Brantingham's (1995) claims regarding the relationships between victims' routine paths and their probability of becoming the victim of crime to cyberspace. Specifically, we believe that as system trespassers are trying to improve the connection and download speed to the target computers (independent of the attackers' physical location), they launch their first system trespassing incidents from IP addresses originating in geographical locations that are proximate to the target computers.

We also find support for the assumption that successful brute-force attacks are more likely to occur during computer networks' most active times (Maimon *et al.* 2013). Specifically, we find that the majority of successful brute-force attacks against the Chinese and Israeli computers took place between 9 am and 5 pm (although the chi-square tests scores and p values were insignificant when analyzing data from the Chinese computers). Interestingly, though we focus on a more advanced stage in the anatomy of system trespassing events (Wilson 2001) and employ a different research design, this finding is consistent with past research (Maimon *et al.* 2013) that indicates that scanning and enumeration activities against a university computer network are more frequent during the university's official business hours. Importantly, this finding further challenges Yar's (2005) assumption that temporal convergence is problematic in cyberspace.

Finally, we find that first system trespassing incidents do not coincide with computer networks' official business hours (Bossler and Holt 2009). Specifically, our findings

suggest that the timing of first system trespassing incidents has little to do with the network users' online routines, and instead, seems to depend solely on trespassers' decisions of when to initiate a trespassing incident. This finding is important because it helps refine our understanding of computer users' responsibilities and ability to prevent different phases in the development of system trespassing incidents. As it turns out, although users' daily online routines and geographical location determine their vulnerabilities during the early stages of an attack, these characteristics are less crucial for the initiation of first system trespassing incidents.

These findings emphasize the need for rethinking the research designs and methods that are commonly used by cyber criminologists to study computer users' and computer networks' vulnerabilities to computer-focused crimes (Furnell 2002) in general, and system trespassing incidents in particular (Maimon *et al.* 2014). Specifically, by studying system trespassing events and preserving the context of cyberspace, one may distinguish between preliminary stages taken by offenders before initiating a system trespassing incident and test the relevance of opportunity theories (Cohen and Felson 1979; Brantingham and Brantingham 1995; Clarke 1995) for the development of successful trespassing events. We suspect that this approach is more valuable and allows greater refinement of our measures (Holt and Bossler 2013), especially compared with asking a respondent to report whether he 'accessed another computer account without [the legitimate user's] knowledge or permission' (Skinner and Fream 1997: 504). At the same time, scholars may assign computer users responsibility for each stage in the attack and explore ways to reduce victims' chances of exposing their computers and networks to different stages in the attack. Most importantly, by developing research designs like the one we described previously, scholars may assess the responsibility of organizations and their IT managers in the development of computer-focused crimes, allowing for more comprehensive theorizing regarding the role of human players (i.e. system trespassers, victims and IT managers) in exposing their network to different types of attacks.

Despite its important theoretical and methodological implications to cyber-criminological research, it is crucial to emphasize that this study, like other context-related studies, is not without limitations. First, we collected data using target computers deployed on the Internet infrastructure of only two educational institutions. Indeed, although the two academic institutions are continents away from each other, they seem to follow similar theoretical patterns. Nevertheless, future research should validate our findings by deploying target computers on the computer networks of other educational, industrial and governmental agencies. Second, we have no way to tell whether system trespassers learned that they were not using legitimate systems with industrial value but rather honeypots that held no industrial value. Related to this, the absence of information regarding system trespassers' technical skills, motivations and resources prevented us from hypothesizing regarding the geographical distribution and timing of *repeated* system trespassing events against our target computers. Specifically, we believe that once compromising a target computer, trespassers can already use the system whenever they want and are less dependent on the victim's routines when accessing the system repeatedly. Therefore, system trespasser's demographic (i.e. gender, age), social (marital and employment status) and personality attributes (i.e. impulsivity) are more important for determining the origin, timing and volume of *repeated* trespassing events against the target computer than the location and time of day on the victimized computer end.

Future research should address this issue and trace system trespassers decision-making processes when repeatedly accessing target computers. Finally, our target computers were set up as computer systems with Linux operating systems, which may limit generalizations from being applied to attackers that target Windows, Mac or other operating systems. Although we have no reason to believe that system trespassers follow different stages of attacks when considering trespassing on computers with a Microsoft environment, this point should be made clear.

In conclusion, this work emphasizes the importance of enhancing our understanding of cyber-victims' susceptibility to cybercrime in general, and system trespassing incidents in particular, by combining existing criminological theories with context-related research designs. Consistent with past criminological research (Sullivan 1989; Wright and Decker 1994), we call for the design of context-embedded studies on victims and cybercriminals. As the Internet establishes a perfect setting for such research designs, we encourage criminologists to explore the wide range of technical tools available for the collection of context-related data and to employ them when theorizing about human behaviours in cyberspace. We believe that such an approach is crucial for the development of a comprehensive theoretical understanding of criminals and victims during different phases of the criminal event, and may facilitate the emergence of interdisciplinary explanations for the occurrence and progression of computer-focused crimes.

Funding

This research was conducted with the support of the Israeli Ministry of Science, Technology and Space (grant number 3-10888) and the College of Behavioral and Social Science at the University of Maryland Dean's Research Award.

Acknowledgements

We thank Tom Holt, David Wall and Fernando Miro for their helpful comments throughout the project.

References

Allen, J. and Stoner, E. (2000), *Detecting Signs of Intrusions*. Software Engineering Institute.

Alston, J. D. (1994), 'The Serial Rapist's Spatial Pattern of Target Selection', doctoral dissertation, School of Criminology/Simon Fraser University.

Ball, D. (2011), 'China's Cyber Warfare Capabilities', *Security Challenges*, 7: 81–103.

Berthier, R. and Cukier, M. (2009), 'An Evaluation of Connection Characteristics for Separating Network Attacks', *International Journal of Security and Networks*, 4: 110–24.

Bossler, A. M. and Holt, T. J. (2009), 'On-Line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory', *International Journal of Cyber Criminology*, 3: 400–20.

——. (2011), 'Malware Victimization: A Routine Activities Framework', in K. Jaishanker, ed., *Cyber Criminology: Exploring Internet Crime and Criminal Behaviors*, 317–46. CRC Press.

Boyd, I. M. (2000), *The Fundamental of Computer Hacking*. SANS Institute.

Brantingham, P. and Brantingham, P. (1991), *Environmental Criminology*. Waveland Press.
——. (1995), 'Criminality of Place: Crime Generators and Crime Attractors', *European Journal on Criminal Policy and Research*, 3: 5–26.
Brenner, S. W. (2010), *Cybercrime; Criminal Threats from Cyberspace*. ABC-CLIO, LLC.
Canter, D. and Larkin, P. (1993), 'The Environmental Range of Serial Rapists', *Journal of Environmental Psychology*, 13: 63–9.
Cheng, N., Wang, X. W., Cheng, W., Mohapatra, P. and Seneviratne, A. (2013), 'Characterizing Privacy Leakage of Public WiFi Networks for Users on Travel', in *INFOCOM, Proceedings IEEE*, 2769–77. IEEE.
Christopher, R. (2001), *Port Scanning Techniques and the Defense Against Them*. SANS Institute.
Clarke, R. V. (1995), 'Situational Crime Prevention', in *Building a Safer Society: Strategic Approaches to Crime Prevention,* edited by Michael Tonry and David P. Farrington. Vol. 19 of *Crime and Justice: A Review of Research,* edited by Michael Tonry. Chicago, IL: University of Chicago Press.
Cohen, L. E. (1981), 'Modeling Crime Trends: A Criminal Opportunity Perspective', *Journal of Research in Crime and Delinquency*, 17: 140–59.
Cohen, L. E. and Felson, M. (1979), 'Social Change and Crime Rate Trends: A Routine Activity Approach', *American Sociological Review*, 44: 588–608.
Demetriou, C. and Silke, A. (2003), 'A Criminological Internet Sting: Experimental Evidence of Illegal and Deviant Visits to a Website Trap', *British Journal of Criminology*, 43: 213–22.
Dodge, M. and Kitchin, R. (2000), *Mapping Cyberspace*. Routledge.
Dodge, M. and Zook, M. (2009), 'Internet Based Measurement', in R. Kitchin and N.Thrift, eds., *The International Encyclopedia of Human Geography*. Elsevier.
Engebretson, P. (2013), *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*. Elsevier.
Erickson, J. (2008), *Hacking: The Art of Exploitation,* 2nd edn. No Starch Press.
Fischer, B. S., Sloan, J. J., Cullen, F. T. and Lu, C. (1998), 'Crime in the Ivory Tower: The Level and Sources of Student Victimization', *Criminology*, 36: 671–710.
Fritzon, A., Ljungkvist, K., Boin, A. and Rhinard, M. (2007), 'Protecting Europe's Critical Infrastructures: Problems and Prospects', *Journal of Contingencies and Crisis Management*, 15: 30–41.
Furnell, S. 2002. *Cybercrime: Vandalizing the Information Society*. Addison-Wesley.
Gadge, J. and Patil, A. A. (2008), 'Port Scan Detection' in *16th IEEE International Conference on Networks*, 1–6.
Garfinkel, S., Spafford, G. and Schwartz, A. (2003), *Practical UNIX and Internet Security*, 3rd edn. O'Reilly Publishing.
Glaser, D. (1971), *Social Deviance*. Markham.
Goldsmith, J. and Wu, T. (2006), *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press.
Hindelang, M. J., Gottfredson, M. R. and Garofalo, J. (1978), *Victims of Personal Crime: An Empirical Foundation for a Theory of Personal Victimization*. Ballinger Publishing Co.
Holt, T. J. and Bossler, A. M. (2009), 'Examining the Applicability of Lifestyle Routine Activities Theory for Cybercrime Victimization', *Deviant Behavior*, 30: 1–25.
——. (2013), 'Examining the Relationship Between Routine Activities and Malware Infection Indicators', *Journal of Contemporary Criminal Justice*, 29: 420–36.

Hutchins, E., Michael, C. and Rohan, A. (2011), 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains'. *Proceedings of the International Conference on Information Warfare*, 113–25.

Johnson, S. D. and Bowers, K. J. 2007. 'Burglary Prediction: The Roles of Theory, Flow and Friction', *Crime Prevention Studies*, 21: 203–23.

Keith, M., Shao, B. and Steinbart, P. J. (2005), 'The Effectiveness and Usability of Passphrases for Authentication'. *Proceeding of the Eleventh Americas Conference on Information Systems*, 3292–5.

Kizza, J. M. (2005), *Computer Network Security*. Springer Inc.

Long, J. (2008), *No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing*, 1st edn. Syngress Publishing Inc.

Maimon, D., Alper, M., Sobesto, B. and 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. and Sobesto, B. 2013. 'Daily Trends and Origin of Computer Focused Crimes against a Large University Computer Network', *British Journal of Criminology*, 53: 319–43.

Marcum, C. D., Higgins, G. E. and Ricketts, M. L. (2010), 'Potential Factors of Online Victimization of Youth: An Examination of Adolescent Online Behaviors Utilizing Routine Activity Theory', *Deviant Behavior*, 31: 381–410.

Mckey, D. (2003), *Web Security for Network and System Administrators*. Cengage Learning.

McQuade, S. C. (2006), *Understanding and Managing Cybercrime*. Pearson Education Inc.

Messner, S. F. and Blau, J. R. (1987), 'Routine Leisure Activities and Rates of Crime: A Macro-level Analysis', *Social Forces*, 65: 1035–52.

Mu, J., Cui, A. and Rao, J. (2013), 'Android Mobile Security–Threats and Protection', in *International Conference on Computer, Networks and Communication Engineering (ICCNCE 2013)*, 683–6. Atlantis Press.

Murnion, S. and Healy, R. G. (1998), 'Modeling Distance Decay Effects in Web Server Information Flows', *Geographical Analysis*, 30: 285–302.

Ponemon Institute. (2013), '*2013 Cost of Cyber Crime Study: United States*', available online at http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf.

Pratt, T. C., Holtfreter, K. and Reisig, M. D. (2010), 'Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory', *Journal of Research in Crime and Delinquency*, 47: 267–96.

Reyns, B. W., Henson, B. and Fisher, B. S. (2011), 'Being Pursued Online: Applying cyber-lifestyle- Routine Activities Theory to Cyberstalking Victimization', *Criminal Justice and Behavior*, 38: 1149–69.

Rossmo, D. K. (1994), 'Targeting Victims: Serial Killers and the Urban Environment', in T. O'Reilly- Fleming and S. Egger, ed., *Serial and Mass Murder: Theory, Research and Policy*. University of Toronto Press.

Salles-Loustau, G., Berthier, R., Collange, E., Sobesto, B. and Cukier, M. (2011), 'Characterizing Attackers and Attacks: An Empirical Study'. *Proceedings of 17th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2011)*, 174–83.

Sampson, R. J. and Lauritsen, J. L. (1990), 'Deviant Lifestyles, Proximity to Crime, and the Offender-Victim Link in Personal Violence', *Journal of Research in Crime and Delinquency*, 27: 110–39.

SANS Institute. (2007), '*SANS Top-20 2007 Security Risks (2007 Annual Update)*', available online at www.sans.org/top20/2007/.

Skinner, W. F. and Fream A. M. (1997), 'A Social Learning Theory Analysis of Computer Crime among College Students', *Journal of Research in Crime and Delinquency*, 34: 495–518.

Snedecor, G. W. and Cochran, W. G. (1989), *Statistical Methods,* 8th edn. Iowa State University Press

Spitzner, L. (2002), *Honeypots: Tracking Hackers*. Addison-Wesley Longman Publishing Co.

Stallings, W. (2005), *Wireless Communications and Networks*. Pearson Prentice Hall.

Sullivan, M. L. (1989), *Getting Paid: Youth Crime and Work in Inner City*. Cornell University Press.

Tanenbaum, A. S. (2003), *Computer Networks,* 4th edn. Prentice Hall.

Thelwall, M. (2002), 'Evidence for the Existence of Geographic Trends in University Web Site Interlinking', *Journal of Documentation*, 58: 563–74.

Vazsonyi, A. T., Lloyd, P. E., Belliston, L. M., Dick, H. and Marianne, J. (2002), 'Routine Activities and Deviant Behaviors: American, Dutch, Hungarian and Swiss Youth', *Journal of Quantitative Criminology*, 18: 397–422.

Wilson, Z. (2001), *Hacking: The Basics*. SANS Institute.

Wright, R. and Decker, S. H. (1994), *Burglars on the Job*. Northeastern University Press.

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

——. (2006), *Cybercrime and Society*. Sage Publications.

Zago-Swart, A. (2001), *How an Exploit in the Computer System of a Small Company was Used to Gain Access to Two Major Government Agencies*. SANS Institute.