# ABSTRACT

Title of Thesis: SURVEILLANCE IN CYBERSPACE: APPLYING NATURAL AND PLACE MANAGER SURVEILLANCE TO SYSTEM TRESPASSING

Lizabeth Paige Remrey, Master of Arts, 2016

Thesis Directed By: Associate Professor David Maimon
Department of Criminology and Criminal Justice

Research on the criminological side of system trespassing (i.e. unlawfully gaining access to a computer system) is relatively rare and has yet to examine the effect of the presence of other users on the system during the trespassing event (i.e. the time of communication between a trespasser's system and the infiltrated system). This thesis seeks to analyze this relationship drawing on principles of Situational Crime Prevention, Routine Activities Theory, and restrictive deterrence. Data were collected from a randomized control trial of target computers deployed on the Internet network of a large U.S. university. This study examined whether the number (one or multiple) and type (administrative or non-administrative) of computer users present on a system reduced the seriousness and frequency of trespassing. Results indicated that the type of user (administrative) produced a restrictive deterrent effect and significantly reduced the frequency and duration of trespassing events.

# SURVEILLANCE IN CYBERSPACE: APPLYING NATURAL AND PLACE MANAGER SURVEILLANCE TO SYSTEM TRESSPASSING

by

Lizabeth Paige Remrey

Thesis submitted to the Faculty of the Graduate School of the
University of Maryland, College Park, in partial fulfillment
of the requirements for the degree of
Master of Arts
2016

Advisory Committee:
Associate Professor David Maimon, Chair
Professor Jean McGloin
Professor Raymond Paternoster

© Copyright by
Lizabeth Paige Remrey
2016

# Table of Contents

# List of Tables

# List of Figures

# Chapter 1: Introduction

Over the last two decades, technology has expanded rapidly and with it has come new opportunities for cybercrime (Kim, Jeong, Kim, & So, 2011; Wall, 2008). In particular, system trespassing (i.e. unlawfully gaining access to a computer system) has become a major problem in the U.S. and worldwide. Large, highly publicized cyber attacks, such as the Ashley Madison hack (Moon, 2015) or the £650 million cyber bank raid (Evans, 2015), have brought system trespassing and its consequences to the forefront of public attention. Despite this, there is still little known about the true extent of system trespassing. In fact, the FBI only recently released its first statistics regarding system trespassing, which report the number of arrests for “criminal computer intrusion”; but because these statistics solely report the number of arrests for system trespassing (105 arrests in 2014), these estimates still fail to elucidate the true extent of the problem (Friedman, 2015).

In addition to difficulties in estimating its prevalence, system trespassing is a relatively untouched area of criminological research. The few criminological studies that do address system trespassing generally look at system trespassing victimization through the lens of Routine Activities Theory (Maimon, Kamerdze, Cukier, & Sobesto, 2013; Pratt, Holtfreter, & Reisig, 2010). On the other hand, other studies examine system trespassing from the trespasser’s point of view (i.e. examining the behavior of the trespasser) (Straub, 1990; Wilson, Maimon, Sobesto, & Cukier, 2015). Notably, few criminological studies of the behavior of the system trespasser address the possible deterrent effects of surveillance of a computer system (Maimon, Alper, Sobest, Cukier, 2014; Wilson et al., 2015). More specifically, research has not yet examined the effect of the presence of other users on the system on the progression of trespassing events (where a trespassing event is the time of communication between the trespasser's system and the infiltrated computer's system [Christensson, 2011]).

Cybercrime research, in general, and on the presence of users on the system, specifically, is of particular interest largely due to its status as a relatively undeveloped area of research. Criminological theories of crime in the physical world (such as Situational Crime Prevention) hypothesize about the impact of the presence of people on crime, and research in accordance with such theories often examines this effect. Thus, research applying criminological theories to the cyber world ought to consider analogous behavior—in this case is the presence of users on the system—to what is researched in the physical world. In the same vein, because criminological research on cybercrime is relatively new, it is important to build a strong theoretical foundation for future research. Therefore, preliminary research (such as this) provides key insight into the applicability of criminological theory to the cyber realm and lays the foundation for future development of a cybercrime paradigm.

With a theoretical basis in Situational Crime Prevention (SCP), Deterrence Theory, and Routine Activities Theory (RAT), this research examines the effects of natural and place manager surveillance on system trespassing. Specifically, this research investigates how the number and type of users on a system affects the number of system trespassing events (i.e. the number of times a trespasser returns to the system), the average time duration of a trespassing event, and the total duration of the trespassing events (i.e. the total time across all events).

# Chapter 2: System Trespassing

The broad term "cybercrime" encompasses a multitude of Internet-based crimes; system trespassing, therefore, is only a single subset of these crimes. One particular definition of cybercrime identifies four sub-categories: cyber-deception or theft, cyber-pornography, cyber-violence, and cyber-trespassing (Wall, 2003). Cyber-deception or theft includes fraudulent use of credit cards and piracy of virtual materials; cyber-pornography is the virtual publication or trading of sexually expressive material; and cyber-violence refers to cyber-stalking and cyber-bullying behaviors (Wall, 2003). This research focuses on cyber-trespassing (also known as system trespassing), which is defined as "the unauthorized crossing of the boundaries of computer systems into spaces where rights of ownership or title have already been established" (Wall, 2003, p. 3). Put another way, system trespassing is unlawfully gaining access to a computer system.

System trespassers can gain access to a system in two ways: by gaining physical access or by gaining remote access via the Internet (Stallings, 2005). Whether physically or remotely, the actual process of gaining access to the system is relatively similar. It begins with the system trespasser gathering information about the target network (i.e. a group of computer systems that are linked together through communication channels) by posing as a legitimate or regular user. Next, the system trespasser will scan the computer network in order to assess possible vulnerabilities for future exploitation and will gather information on system users' accounts (including their account passwords). Then, the trespasser will attempt to enter the system by exploiting the vulnerabilities, while simultaneously attempting to crack users' passwords. And finally, if this is successful, the trespasser will gain access to the system (Maimon, Wilson, Ren, & Berenblum, 2015; Wall, 2003).

Since system trespassers often attempt to hide or disguise their online activities, it is very difficult to detect a system trespasser on a computer (Wall, 2003). Additionally, similar to crime in the physical world, system trespassing often goes unreported (Esterbrook, 2002). In fact, a 2002 survey by the Federal Bureau of Investigation (FBI) found that only 34% of companies that detected system trespassing actually reported those incidents to authorities (Esterbrook, 2002). Consequently, analogous to using arrest reports to estimate prevalence of various crimes in the physical world, using official reports of system trespassing is likely not an accurate representation of the phenomenon.

However, despite such difficulties, there are still quite a few reports that attempt to estimate the prevalence of system trespassing. For instance, a 2005 study by the Bureau of Justice Statistics reported that two-thirds of U.S. businesses detected at least one cybercrime on their system (Bureau of Justice Statistics, 2005). By 2014, according to the U.S. State of Cybercrime Survey, the number of businesses detecting system trespassing incidents increased to three-fourths (77%) (Mickelberg, Pollard, & Shive, 2014). Additionally, the Ponemon Institute estimated that, during the 2015 U.S. fiscal year, the average loss for companies due to data breaches from system trespassing exceeded $15 million (a 19% increase from 2014); while worldwide, the average loss exceeded $7.7 million in 2015 (Ponemon Institute, 2015). Despite the high rate of under-reporting of system trespassing, these losses due to system trespassing are still incredibly high, indicating that the true loss is likely even greater.

Consequently, companies have taken to using certain measures to detect, prevent, and mitigate system trespassing. Intuitively, quick detection of a system trespassing event is an important way to minimize damage (Rubens, 2015). However, since detection of system trespassing is incredibly difficult (Wall, 2003), some Information Technology (IT) managers, as well as the National Institute for Standards and Technology, suggest focusing efforts on prevention and mitigation techniques. For example, Homeland Security uses National Cybersecurity Protection System (NCPS) and Continuous Diagnostics and Mitigation (CDM) to secure federal networks by preventing intrusions, detecting intrusions early, prioritizing intrusions based on potential impact, and enabling personnel to mitigate the system trespass (Homeland Security, 2015).

On the individual company level, IT officers propose many options for increasing system security in order to prevent system trespassing events, including having password protection, changing passwords regularly, encrypting or disguising files, and physically disconnecting important systems from corporate networks (Brumfield, 1999; Farhat, McCarthy, & Raysman, 2011; Rubens, 2015). However, understandably, complete prevention can never be achieved. As in the physical world where no crime prevention measures will fully stop the commission of crimes, no cyber-related prevention techniques will completely stop the occurrence of system trespassing. Thus, in order to reduce the potential damaging outcomes of system trespassing, minimizing or mitigating trespassing events becomes vitally important.

Mitigation techniques often involve surveillance of the computer system. Such surveillance can be accomplished via automated processes or manually by humans. Automated processes include intrusion detection and prevention systems (IDS/IPS) that scan and analyze networks, recognize threats, and then either send alerts about the detection or automatically deal with the detected threat according to predetermined protocols (Huey & Rosenberg, 2004; Mueller & Kuehn, 2013). Additionally, some companies monitor the activities of individuals on their systems by employing programs that capture information on their employees' activities (e.g. searching employee work files, e-mails, network messages, and voicemails) (Moore, 2000). On the other hand, some surveillance is done in a less sophisticated way via manual surveillance. Smaller companies may simply employ an individual to manually sift through users' activities and files looking to identify anything suspicious. This method is much more tedious, which means that not all activity is examined (that is simply not feasible) but all activity has the *potential* to be examined.

Overall, the motivation behind monitoring the activities on a computer system is twofold: first, any system trespassing incidents can be detected and eliminated early; and second, system trespassers who are aware of the surveillance may reduce the seriousness of their trespassing events in order to avoid detection. Both of these goals work to reduce the amount of time a system trespasser spends on the system, thereby reducing the amount of damage the trespasser can inflict. These goals of mitigating system trespassing are very similar to goals drawn from Situational Crime Prevention, Routine Activities Theory, and Deterrence Theory and the subsequent approaches that are used to mitigate crime in the physical world.

# Chapter 3: Theoretical Import

## *3.1 Situational Crime Prevention*

Situational Crime Prevention (SCP) was first introduced by Ronald Clarke in 1980. As opposed to traditional theories of crime, which focus on the disposition (biological, psychological, or sociological) of the offender, Clarke's (1980) idea focuses on the situational aspects of crime as well as on crime as an outcome of choices of the offender. In this way, SCP has a theoretical foundation in both Rational Choice Theory (Cornish & Clarke, 1986) and Routine Activities Theory (Cohen & Felson, 1979). The Rational Choice Theory aspect of SCP emphasizes that the process of offender decision-making is rational (i.e. intended to benefit the offender) and is constrained by time and available information (Cornish & Clarke, 1986). The Routine Activities Theory (RAT) facet of SCP focuses on the environmental component of crime, stating that the convergence of three elements is necessary for crime to occur: a motivated offender, a suitable target, and lack of a capable guardian[1] (Cohen & Felson, 1979). Combining the decision-making aspect of Rational Choice and the situational context of Routine Activities provides the general basis for SCP. Clarke (1980) asserts that the components that play a part in an individual's decision to commit a crime will be "influenced by immediate situational variables and by highly specific features of the individual's history and present life circumstances" (p. 138).

[1] RAT is not wholly applicable to this research because this work does not consider all three of its core elements. This work does, however, examine the surveillance components of SCP, which remain consistent with the guardianship element of RAT, as will be discussed later in this paper.

Due to its dual focus on situational context and offender decision-making, SCP proposes that crime prevention can be attained by manipulating criminogenic situations in order to make them less attractive to a potential offender (Clarke, 1980; Clarke, 1995). These prevention recommendations fall into five categories—increase effort, increase the risks, reduce the rewards, reduce provocations, and remove excuses (Cornish and Clarke, 2003). For each category, Cornish and Clarke (2003) identified five concrete techniques (providing 25 crime prevention recommendations[2]), which are assumed to be effective in mitigating or reducing the development of criminal events.

### ***3.2 Restrictive Deterrence as an Outcome of SCP***

The idea of reducing the development of criminal events is not unique to SCP, but is echoed in new theoretical developments of one of the classic theories of crime—Deterrence Theory. Deterrence Theory posits that crime deterrence occurs when the perceived risk and fear of formal, legal punishment for an act results in the omission of that act, where the risks and fear of punishment consist of the perceived certainty, severity, and celerity of the punishment (Gibbs, 1975). In other words, if the risk of punishment is enough to counteract the benefits of the crime, then it will result in deterrence from crime. Alternatively, if the risk of punishment is not enough to counteract the benefits of the crime, then there will be no deterrent effect. However, recent advancements in Deterrence Theory have come to acknowledge

[2] Cornish and Clarke's (2003) SCP tactics: (1) increase the effort (target harden, control access, screen exits, deflect offenders, control tools/weapons); (2) increase the risks (extend guardianship, assist natural surveillance, reduce anonymity, utilize place managers, strengthen formal surveillance); (3) reduce the rewards (conceal targets, remove targets, identify property, disrupt markets, deny benefits); (4) reduce provocations (reduce frustrations and stress, avoid disputes, reduce emotional arousal, neutralize peer pressure, discourage imitation); (5) remove excuses (set rules, post instructions, alert conscience, assist compliance, control drugs and alcohol).

additional outcomes other than the do-or-don't commit crime dyad, specifically differentiating between absolute and restrictive deterrence (Gibbs, 1975; Jacobs, 2010).

Absolute deterrence involves wholly refraining from a particular type of criminal act because of a perceived risk of punishment; while restrictive deterrence describes the "curtailment of a certain type of criminal activity" due to fear of punishment (Gibbs, 1975). In other words, where absolute deterrence involves an individual abstaining from crime for the rest of his or her life, restrictive deterrence involves a reduction in the frequency with which a crime is committed for someone who has already committed the crime at least once (Gibbs, 1975). In order to expand the scope of this concept, Jacobs (2010) elaborated further that restrictive deterrence could also result in modification of the initial crime. Such modification includes reducing the seriousness of the crime, modifying the behaviors in order to reduce the risk of detection (e.g. wearing a mask to avoid identification), and altering the spatial-temporal component of the criminal event (Jacobs, 2010). In particular, three of these dimensions of restrictive deterrence (reduce frequency, reduce seriousness, and modifying behaviors to reduce the risk of detection) are consistent with SCP's goals of reducing the progression of criminal events.

Overall, SCP proposes that opportunity-reducing measures that are focused on a specific form of crime, that manipulate the immediate environment, and that make crime more risky or less rewarding can aid in crime mitigation (Clarke & Cornish, 1985; Cornish & Clarke, 1986). Combining this with theoretical developments of

Deterrence Theory leads to the conclusion that SCP opportunity-reducing measures have the potential to result in restrictive deterrence.

### ***3.3 Increasing the Risks of Crime via Surveillance***

One of the original strategies proposed by Clarke (1980) to reduce the occurrence of crime involves the introduction of surveillance means. Surveillance in SCP is relatively analogous to the presence of a capable guardian in RAT (Felson, 1995). Both guardianship and surveillance propose the "physical or symbolic presence" of one or multiple individuals whose mere presence increases the potential of an offender being detected and, therefore, increases the risk of the crime (Hollis-Peel, Reynald, van Bavel, Elffers, & Welsh, 2011). Thus, the introduction of guardians and surveillance means serve to mitigate crime by increasing offenders' perceived threat of detection and punishment.

Clarke and Homel (1997) identify three types of surveillance: natural surveillance, formal surveillance, and surveillance by place managers. Natural surveillance is commonly associated with Crime Prevention Through Environmental Design (CPTED[3]) (Erickson & Houck, 2005), but is also a technique of SCP. Natural surveillance involves manipulating the physical environment to improve everyone's ability to see what is going on, which increases the chance of an offender being seen or detected and reduces the likelihood of crime (Erickson & Houck, 2005). This can

[3] CPTED is a crime prevention strategy intended to decrease the opportunity and the likelihood of crime by manipulating the layout of physical space. The four main tenets are natural surveillance, natural access control, territorial reinforcement, and maintenance (Erickson & Houck, 2005). Natural surveillance is the idea of "see and be seen," where lighting and landscape improve users' abilities to see what is going on; natural access control involves the use of walkways and fences (among other things) in order to guide the flow of people; territorial reinforcement involves clear indication of what is public and what is private space and enabling users of the space to have a sense of ownership and control over it; and maintenance is the idea of maintaining properties (Erickson & Houck, 2005).

be accomplished by improving street lighting and promoting the "see something, say something" agenda.  Formal surveillance is the idea of increasing official forms of crime prevention personnel and hardware (Clarke, 1997).  This includes police presence, security guards, CCTV, red light cameras, and burglar alarms.  Lastly, surveillance by place managers (i.e. place manager surveillance) involves using employees who already have a responsibility to monitor conduct to also fulfill a surveillance role (Clarke, 1997).  Such personnel include building attendants, concierges, park keepers, train conductors, and convenience store clerks.

# Chapter 4: Outcomes of Situational Crime Prevention

There is a substantial amount of literature applying Situational Crime Prevention to various crimes—including robberies (convenience store and fast-food restaurant) (Exum, Kuhns, Koch, & Johnson, 2010), barroom violence (Graham, 2009), street crime (Painter & Farrington, 2001), worldwide piracy (Shane, Piza, & Mandala, 2015), retail theft (Hayes, Downs, & Blackwood, 2012), environmental offenses (Huisman & van Erp, 2013), organized crime (von Lampe, 2011), and terrorism (Weenink, 2012), among others. Overall, such research finds a significant relationship between the application of SCP tactics and a reduction in various types of crime (Exum et al., 2010; Hayes et al., 2012; Huisman & van Erp, 2013; Painter & Farrington, 2001; Shane et al., 2015). In fact, Eck (1997), in a review of literature testing Situational Crime Prevention, found largely positive results across a number of crime types. Approximately 90% of the evaluated interventions resulted in crime reductions (Eck, 1997). From this, Eck (1997) concluded that Situational Crime Prevention tactics that are aimed at specific crimes in specific places hold promise for crime reduction.

## ***4.1 Surveillance in the Physical World***

More relevant to this work, there are some studies that test the applicability of particular aspects of SCP, such as the surveillance tactics within the SCP category of increasing the risks of crime. For example, Painter and Farrington (2001) found that increasing the amount of street lighting, which increases an offender’s risk of being seen and/or caught (i.e. assisting natural surveillance), reduced violent crime after dark. In another study, Welsh and Farrington (2004) compared the effects of CCTV (formal surveillance) with those of improved street lighting (natural surveillance) on crime in public spaces. Their results indicated that both techniques were effective in reducing crime (Welsh & Farrington, 2004). More specifically, improved street lighting was more effective in city centers (than was CCTV) and both surveillance types were more effective in reducing property crimes rather than violent crimes (Welsh & Farrington, 2004). In a meta-analysis of the effectiveness of CCTV, Welsh & Farrington (2009) found that CCTV was effective in reducing crime, but this was largely driven by its high efficacy in car parks and on public transport, elsewhere the effects were modest.

Less common in research is a focus on place manager surveillance. One such study examines the importance of the behavior and decisions of a bar manager in determining whether or not violence will occur in that bar. Madensen and Eck (2008) hypothesized that managers, not just the crime-rate and other neighborhood characteristics, could have an effect on the amount of violent crime in a bar. Their research supported this hypothesis and highlighted the important role the place mangers play in reducing crime. Madensen and Eck (2008) concluded that managers can "create settings that can suppress the effect of outside influences" or they can "create environments that permit or encourage violent behavior regardless of contextual characteristics" (p. 122).

In particular, research on the deterrent effect of surveillance techniques on burglary is especially applicable to this research because burglary is often considered the physical world counterpart to system trespassing. Burglary is defined as "entering a building without being authorized to do so" with the intent to commit an offense; while system trespassing is defined as gaining access to a computer system without authorization for the purpose of committing a crime (Brenner, 2010, p. 50). Within their definitions, there are clear parallels between burglary and system trespassing. Despite sometimes dramatic differences between the respective physical and cyber domains for burglary and system trespassing, we can still guide inquiry into system trespassing based upon insight derived from the former. One study in particular by Wilcox, Madensen, and Tillyer (2007) examined the effects of natural and place manager surveillance on burglary victimization. The results suggested that natural surveillance (in the form of the physical layout of the space) and place manager surveillance (in the form of homeowner occupancy) both decreased the likelihood of burglary victimization (conditional on neighborhood surveillance factors) (Wilcox et al., 2007). Overall, past research on surveillance in the physical world shows support for all three forms of surveillance (natural, place manager, and formal) as techniques to reduce various types of crime.

## ***4.2 Situational Crime Prevention in Cyberspace***

The application of SCP to system trespassing is a relatively new endeavor, which comes with its own challenges (namely, applying a theory that is quite enmeshed in the physical world to the cyber world). Accordingly, there is a dearth of research empirically testing the application of SCP principles in the context of system trespassing. For instance, Maimon et al. (2014) found that presenting a warning banner providing a threat of sanction (i.e. removing the excuses of the crime) at the time of entry into a hacked system reduced the duration of system trespassing events (see also Stockman, Heile, & Rein, 2015). Similarly, Wilson et al. (2015) found that a surveillance banner indicating formal surveillance and monitoring of the system (i.e. increasing the risks of the crime) displayed at the time of entry to a hacked system reduced the probability of commands being entered on the system for trespassers who were on the system longer.

However, as of yet, there is no empirical research examining how the presence of users on the system influences the progression of system trespassing events. In fact, unlike burglary in the physical world, there has not yet been any research examining natural or place manager surveillance in cyberspace. Addressing these gaps, this study seeks to determine whether the number (one or multiple) and type (administrative or non-administrative) of users on the system will influence the progression of a system trespassing event.

# Chapter 5: The Present Study

This thesis examines the surveillance and guardianship aspects inherent in SCP and RAT, particularly investigating the effects of natural surveillance and place manager surveillance on system trespassing. As previously discussed, in the physical world, natural surveillance is the ability of people to see and be seen. Natural surveillance in the physical world is often associated with improving the street lighting or manipulating the layout of the physical environment in some way that improves visibility. In the cyber world, natural surveillance can be considered the ability of users on a system to see the actions of other users. These users are the average, everyday users of the system (i.e. non-administrative users) and do not hold any special duties, administrative or otherwise (the equivalent of a regular citizen in the physical world). Unlike in the physical world, there is no physical environment to manipulate in cyberspace. Instead, the number of users present on a system can affect the ability to see other users' actions. The larger the number of users on a system, the more activity is present on the system, and the more difficult it is for an administrative user to sift through that activity in order to identify suspicious behavior or unauthorized users. Alternatively, the fewer the number of users on a system, the less activity on the system and the easier it is for an administrative user to be alert for and identify suspicious behavior.

In the physical world, place manager surveillance involves the manager of a specific place taking on a surveillance role in addition to his/her current monitoring role. The most common example of a place manager is a convenience store clerk. Clerks are in charge of customer service and helping the patrons of the store; but, additionally, they may be charged with surveillance of the store, where they are also expected to keep an eye on the store and make sure nothing suspicious or nefarious happens. In cyberspace, a place manager is equivalent to an administrator of a system (someone who has more responsibility and power than a regular user) taking on the additional role of surveillance on the system. In this case, the user has administrative power on the system because of their employment position, and due to that extra power they also have the ability to oversee the actions of the other users on the system and be alert for system trespassers. Thus, if a system trespasser perceives either kind of surveillance on the system (natural or place manager), he/she may fear detection and reduce the progression of the system trespassing incident.

In accordance with SCP and restrictive deterrence, reducing the progression of a system trespassing event can be measured by the frequency and seriousness of the crime. In this context, the frequency and seriousness of system trespassing is measured in three ways: the number of times a trespasser returns to the system (number of repeat trespassing events), the average duration of a system trespassing event, and the total duration of all system trespassing events. It is expected that surveillance, indicating an increased risk of detection, will result in a trespasser reducing the amount of time he/she spends on the system (in total and on average per trespassing event) and reducing the number of times he/she returns to the system.

## ***5.1 Hypotheses***

Accordingly, this research proposes six hypotheses. It is expected that the presence of an administrative user (i.e. a place manager), as a result of their position of greater ability to detect a system trespasser, will increase the risk of detection and, therefore, reduce the progression of system trespassing. Thus, *the presence of an administrative user on the attacked system (compared to a non-administrative user)* (1a) *will reduce the number of repeated system trespassing events;* (1b) *will reduce the average duration of a system trespassing event; and* (1c) *will reduce the total duration of all system trespassing events*.

Additionally, it is expected that the presence of a greater number of computer users on the attacked system will provide protection from detection (because of the increased amount of activity on the system) and will prompt the progression of a system trespassing event. Thus, *the presence of multiple users on the system (compared to one user)* (2a) *will result in a greater number of system trespassing events;* (2b) *will result in a longer average duration of a system trespassing event; and* (2c) *will increase the total duration of all system trespassing events.*

# Chapter 6: Data and Methods

This research tests these hypotheses using system trespassing data collected from a randomized control trial of target computers (i.e. honeypots) deployed on the Internet infrastructure of a large U.S. academic institution in order to be attacked. Target computers are “virtual or physical hosts used for the sole purpose of collecting malicious activity” (Cukier, Maimon, & Berthier, 2012, p. 27). The activity detected on the target computers is suspect by nature (and deemed “malicious”) because target computers have no value and therefore there is no reason for a legitimate user to communicate with them (Spitzner, 2003). Thus, all the activity collected from a target computer can be reasonably assumed to be the activity of system trespassers. Furthermore, target computers are a passive entity, meaning they do not entice system trespassers to infiltrate the system, but rather they allow a trespasser to initiate a system trespassing event on his/her own accord (Spitzner, 2003). Therefore, the information collected from target computers is unique in that it is likely an accurate representation of the activities system trespassers actually engage in when on a compromised system.

## ***6.1 Experimental Design***

This research uses data collected from target computers deployed on a U.S. university network to be attacked. The deployment of the target computers is depicted in Figure 1. As Figure 1 shows, each new trespasser IP address[4] is assigned its own target computer, all of which are connected to the same network.

[4] IP addresses are the public identification numbers assigned to computers that allow computers to connect to the internet and to interact with one another.

Over the deployment period, the target computers captured the movements of any trespassers that infiltrated their systems. In order to gain access to the system, the system trespassers had to guess (or crack) the passwords of the system's "legitimate users" (Maimon et al., 2015), usually using brute-force techniques, such as programs that are built for cracking passwords (McQuade, 2006). The target computers were structured to deny a trespasser access until an $n^{th}$ try (where n was a randomized number between 100 and 200). Upon attempting access the $n^{th}$ time, the trespasser would be allowed access to the system and the $n^{th}$ login credentials would be treated as legitimate credentials for that trespasser moving forward. System trespassers were identified and connected to their fake system credentials by their IP addresses. Therefore, once a particular IP address gained access to the system, it was allowed access only under its unique credentials. By attaching unique credentials to each system trespasser's specific target computer, it is most likely that anyone who subsequently used those credentials to access that target computer was the same trespasser. And by identifying system trespassers via their IP addresses, each system trespasser was assigned his/her own target computer and was only exposed to one experimental condition. However, system trespassers who manipulated their IP addresses could gain access to the system under different credentials and potentially be exposed to different conditions, ramifications of which will be discussed in the limitations section.

System trespassers were allowed to re-access the system using that same login and password for 30 days, meaning the trespassers could engage in multiple trespassing events during the 30-day period that the system was opened to them. In other words, after a trespasser brute-forced his/her way into the system and attained login credentials, they had to return to the system and use those credentials to log in in order to actually begin a trespassing event on the system. Additionally, trespassers could open more than one line of communication at a time (similar to opening multiple tabs of a web browser), meaning more than one trespassing event could occur simultaneously. After 30 days, the trespasser was blocked from entering, the system was cleaned, and the target computer was redeployed to be attacked again. Figure 2 describes and visually represents this process. It is important to keep in mind that this process occurs for each new IP address or trespasser that attempts to infiltrate the target computer system.

Upon gaining access to the system, the target computer for the system trespasser was randomly assigned to the control group or one of four treatment conditions. The assigned condition was associated with the number and type of fake users that would appear to be on the system at the same time as the system trespasser. The control did not have any additional users on the system. The first treatment condition had one non-administrative user on the system; the second treatment condition had one administrative user on the system; the third treatment condition had ten non-administrative users; and the fourth treatment condition had nine non-administrative users and one administrative user. In the interest of parsimony, the conditions will be referred to as one user (no administrator), one user (administrator), multiple users (no administrator), and multiple users (administrator), respectively. For reference, Table 1 provides the names of each condition as well as the number and type of users assigned to the condition.

For all of the treatment conditions, the fake users cycled on and off the target computer system on eight-hour, offset intervals, so that the treatment conditions would always have the same number and type of users according to the random condition originally assigned to the system trespasser's target computer, but the users themselves would not be the same (as evidenced by their system username). For example, if a system trespasser was randomly assigned to one user (no administrator), then at all times there would appear to be a single non-administrative user on the system, but every eight hours the username of that user would change so as to imitate the natural movement of users logging in and out of a system. In other words, it would appear as though a different user had logged onto the system, but, regardless, the system trespasser was always exposed to that same condition.

The data for this thesis come from seven (non-consecutive[5]) months of the captured movements of trespassers on the target computers, collected between July 2014 and March 2015. Over this time, 448 trespassers gained access to target computers and 6,179 total system trespassing events were initiated against those target computers. The data collected include information on the system trespassing events (e.g. the number of trespassing events, the duration of the events, etc.), the IP address of the trespasser, the username of the trespasser, and the randomly assigned treatment condition of the trespasser's target computer.

[5] There were some months during the data collection period during which no target computers were infiltrated. Consequently, this study utilizes seven months of recorded trespassing events and does not consider the months during which no events were recorded.

### ***6.2 Outcome Measures***

The dependent variables for this thesis are the number of system trespassing events (a count variable indicating the number of trespassing events each system trespasser had on the system), the average duration of the trespassing incident (a continuous variable indicating the average amount of time the trespasser was on the system per event, measured in minutes[6]), and the total amount of time the trespasser spent on the target computer (a continuous variable also measured in minutes). Initial analysis of these variables uncovered two issues. First, for the number of system trespassing events, 197 trespassers had zero system trespassing events. This indicates that a system trespasser gained access to the system, but after receiving the fake system credentials did not return to the system and begin any trespassing events. Because this analysis is focused on the effect of surveillance on users who actually began trespassing events, the observations with zero events were dropped from the final analysis, bringing the number of trespassers to 251.

Second, a similar issue existed with the average duration of the trespassing event and total duration of the trespassing events. Some trespassers who did begin trespassing after gaining access to the system had trespassing events that lasted zero seconds. This could be the result of a trespasser who began an event but immediately stopped (allowing the system to acknowledge that the trespasser logged on, but resulting in an event that lasted zero seconds). Alternatively, this may have been a glitch in the program that resulted in no time being recorded for those trespassing

[6] Data on the average duration of the system trespassing events were originally collected in seconds. However, the long periods of time many trespassers spent on the system made for nonsensical and difficult interpretations when reported in seconds. To remedy this, the duration variable was divided by 60, producing a continuous variable indicating the average number of minutes a trespasser spent on the system per trespassing event.

events. As with the observations with zero events, trespassers that had trespassing events of zero time were removed from the analysis, resulting in 239 system trespassers. The exclusion of the zero event and zero time observations affected the distribution of the experimental conditions in an unexpected way. Table 2 shows the distribution prior to excluding the two types of zeros and after excluding first the zero event observations (n=197) and then the zero time observations (n=12). As the table indicates, the trespassers that had zeros were more likely to be those assigned to target computers with one user (administrator) or multiple users (administrator).

Recognizing the potential consequences of these unevenly distributed zero observations, diagnostics were run in an attempt to explore and understand differences in the composition of the zero observations. I examined the distributions of the types of system trespassers that gained access to the system. Specifically, I looked at the distribution of administrative usernames used by the system trespassers to access the system in each condition.[7] System trespassers choose the username they are going to attack at the beginning of the attack, before they would be randomly assigned to any of the experimental conditions. As such, this distribution should be evenly distributed across the experimental conditions due to random assignment. Disparities in the distribution of usernames would indicate the presence of an underlying bias impacting which system trespassers were in the zero observations. Table 3 shows the distribution of administrative system trespassers across the experimental conditions for the sample that includes all zero observations (n=448) and for the sample that excludes all zero observations (n=239). For the full sample,

[7] System trespassers are capable of gaining access to the system as an administrative user or as a regular user (e.g. non-administrator). Gaining access as an administrator gives a trespasser more power over the system and allows for greater manipulation of the system.

the percent of observations that were administrative trespassers ranges from approximately 85% to 89%; and the reduced sample has between 90% and 98% administrative trespassers, depending on the condition. As indicated in Table 3, the exclusion of the zero observations increased the proportion of administrative trespassers across all conditions. This effect is largest for the one user (no administrator) and multiple users (no administrator) conditions, increasing the proportion by 9% and 10.5%, respectively. The remaining conditions (control, one user [administrator], and multiple users [administrator]) increase between 3% and 6%.

Additionally, Table 3 shows that the overall percentage of administrative trespassers is 88% in the full sample and 95% in the reduced sample. Although this indicates an increase in the proportion of administrative system trespassers, on the whole these proportions are still quite high and relatively similar. Thus, the exclusion of the zero event and time observations does not appear to be considerably altering the composition of the sample in terms of the system trespasser user type.

Initial analysis of the number of system trespassing events also indicated the existence of potential outliers on the high end of the number of trespassing events distribution. First, all observations with greater than 200 trespassing events (four observations) were removed because they were quite far from the remainder of the distribution and likely would have had undue influence on the results. Next, there was one observation (139 trespassing events) that was uncertain as to whether it was too far from the distribution. The analysis was conducted with and without this observation and the findings showed that the observation was substantively changing the outcome; therefore, it was removed from the final analysis. Ultimately, five outlying observations were removed due to concerns for their influence on the results. After accounting for the zeros and outliers, the final number of observations was 234 trespassers who initiated a total of 4,517 trespassing events. Figures 3, 4, and 5 show the final distributions for the number of trespassing events, the average duration of the event, and the total duration of the system trespassing events, respectively. As the histograms indicate, the distributions of the outcome variables are right skewed, consequences of which will be discussed later.

Table 4 shows the descriptive statistics for the number of system trespassing events, the average duration of the event, and the total duration on the system for the sample. It indicates that the average number of trespassing events is just less than 20 incidents, with a minimum of 1 incident and a maximum of 108 incidents. Additionally, Table 4 shows the average duration per trespassing event ranges from 0.01 minutes to 78.61 minutes, with a mean of 13.83 minutes. Lastly, the total duration of trespassing events has a mean of 151.94 minutes (about 2 and one half hours) and ranges from .02 minutes to 1021.88 minutes.

Table 5 depicts the number of system trespassers, the total number of trespassing events, the average number of events per trespasser, the average mean duration of events per trespasser, and the average total duration per trespasser for each experimental condition. The number of trespassers assigned to each experimental condition ranges from 21 (multiple users [administrator]) to 67 (one user [no administrator]).

## ***6.3 Methods***

In order to determine whether the presence and type of other users on a system has an effect on the progression of the system trespassing event, this research examined whether there was a difference in means between the experimental conditions for the total number of system trespassing events, average duration of the system trespassing event, and total duration of the trespassing events. Experimental data lends itself to answering these questions because potential unobserved heterogeneity across treatment groups is mitigated with random assignment, making the groups balanced on expectation for observables and unobservables. In other words, a randomized control trial provides confidence that the differences in the outcomes are due to the treatment. This research tested the hypotheses in two steps: first by utilizing one-way analysis of variance (ANOVA) in order to determine if there was a difference in means for at least one of the experimental conditions; second, if there was a difference in means, by using post hoc Tukey tests[8] to examine which conditions had significantly different means.[9]

[8] The post hoc Tukey test is favorable here over a normal pairwise t-test because it controls for the Type I error rate (or the inflation of alpha) that occurs when doing multiple comparisons across groups.

[9] ANOVA is an omnibus test, where the null hypothesis is that all group means are equal. Therefore, a rejection of this null hypothesis only indicates that at least one group mean is significantly different, but does not indicate how many are different or specifically which ones are different. The second stage of testing, using post hoc Tukey tests, compares across all possible pairings of group means and indicates specifically which means are significantly different.

# Chapter 7: Results

## *7.1 Number of Trespassing Events*

I began my analysis by testing the hypotheses regarding the number of repeated trespassing events (1a and 2a). Table 6 reports the analysis of variance results.[10] Here, the null hypothesis was that there were no differences between the average numbers of repeated trespassing events across the experimental conditions. With a p-value less than .01 (p=0.0000) and an F statistic of 7.70, I reject the null hypothesis, indicating that at least one mean was significantly different from the others. Additionally, Table 6 reports the eta-squared[11] value for this ANOVA. The eta-squared indicates that approximately 11.9% of the variance in the number of trespassing events is explained by the experimental condition assignment. The second step for testing these hypotheses examined which means were different across the experimental conditions using post hoc Tukey tests.

Table 7 shows the results for whether the presence of administrative users compared to non-administrative users on the system reduced the number of trespassing events (Hypothesis 1a). To test this, I analyzed the comparisons according to presence of an administrative user on the system, while controlling for the number of users on the system. This resulted in two tests: one between the one user (administrator) and one user (no administrator) conditions, and the other between the multiple users (administrator) and multiple users (no administrator) conditions.

[10] Due to the skewed distributions of the three outcome variables (violating the normality assumption of ANOVA), the Kruskal-Wallis H-test was also performed. The Kruskal-Wallis H-test is a non-parametric test with relaxed normality assumptions. The results of this test were in agreement with the results of ANOVA, so ANOVA is used and reported for this analysis.

[11] Eta-squared is a measure of the effect size of the independent variable on the dependent variable. It is calculated as a ratio of the explained sums of squares divided by the total sums of squares.

Table 7 indicates that trespassers assigned to target computers with one user (administrator) had significantly fewer trespassing incidents than those assigned to one user (no administrator). In fact, trespassers who had the one user (administrator) condition had (on average) almost 20 fewer trespassing incidents than those that had one user (no administrator) on the system (4.33 trespassing incidents versus 23.82, respectively). Additionally, trespassers assigned to target computers with multiple users (administrator) had significantly fewer trespassing incidents (about 22 less) than those with multiple users (no administrator) (4.43 trespassing incidents compared to 26.72, respectively). Because these means are significantly different, it appears that the presence of administrative users, as opposed to non-administrative users, reduced the number of trespassing events, which provides support for Hypothesis 1a.

Hypothesis 2a (whether a greater number of users on the system increases the number of trespassing events) was tested by analyzing comparisons according to the number of users on the system, controlling for the type of users on the system. This too resulted in two tests: one between multiple users (no administrator) and one user (no administrator), and the second between multiple users (administrator) and one user (administrator). As Table 7 indicates, there were no significant differences in the number of trespassing events for either of these comparisons. This lack of significance does not necessarily disprove Hypothesis 2a, but it also does not find support for it. Thus, it does not appear that the number of fake users on the system had an effect on the number of system trespassing events by trespassers.

The results in Table 7 further illustrate the lack of effect of the number of users on the system on the number of trespassing events. This is evidenced by the similar magnitude of effect for the type of user, regardless of the number of users. For example, system trespassers who had one user (administrator) on the system versus those with one user (no administrator) had nearly 20 fewer trespassing incidents; while system trespassers with multiple users (administrator) versus those with one user (no administrator) also had almost 20 fewer trespassing incidents. Therefore, compared to having one user (no administrator) on the system, whether the system trespasser had a target computer with one user (administrator) or multiple users (administrator) had no different effect on the number of trespassing events. Similarly, system trespassers assigned to one user (administrator) versus multiple users (no administrator) had approximately 22 fewer trespassing events; and those assigned to multiple users (administrator) also had 22 fewer trespassing events compared to those assigned to multiple users (no administrator).

Additionally, Table 7 shows significant differences between one user (administrator) versus control and multiple users (administrator) versus control. Both of these comparisons show that trespassers on target computers with an administrative user (regardless of the number of users) had significantly fewer trespassing events (14 fewer) compared to trespassers on target computers with no users present. Combining this finding with the findings of the significant differences between trespassers with administrative users and those with non-administrative users, I find that where trespassers on target computers with administrative users had 14 fewer trespassing incidents than those on control target computers (4 trespassing events versus 18), trespassers assigned to administrative users had 20-22 fewer trespassing incidents than those assigned to non-administrative users (4 trespassing events versus 24-26), regardless of the number of users on the system. This indicates that trespassers assigned to administrative users had the least trespassing incidents and trespassers assigned to non-administrative users had the most, with the control assignment falling in the middle. Not only does this agree with the previous finding that it is the type of user over the number of users that is of most importance, but this also indicates that the presence of non-administrative users may in fact *increase* the number of trespassing events compared to having no users on the system or having an administrative user on the system.

### ***7.2 Average Duration of Trespassing Event***

The next two hypotheses (1b and 2b) tested the effects of the number and type of users on the average duration of the trespassing event per trespasser. The ANOVA results for the first stage of testing the average duration are shown in Table 8. The analysis of variance for average duration of the trespassing event is not significant with an F statistic of 1.47 (p>.05). Thus, I fail to reject the null hypothesis of the ANOVA and conclude there were no significant differences in means between the groups. Additionally, the eta-squared value of 0.025 indicates that the experimental condition only explained about 2.5% of the variance in the average duration of the event, which is expectedly small given the lack of significance.

Because I fail to reject the null hypothesis, the next step for evaluating this set of hypotheses is not necessary, and I fail to find support for Hypotheses 1b and 2b. Therefore, it appears that neither the number of users nor the type of users on the system had an effect on trespassers' average duration of the system trespassing event.

### *7.3 Total Duration of System Trespassing Events*

Hypotheses 1c and 2c tested the effects of number and type of users on the total duration of the system trespassing events. The analysis of variance for this relationship is presented in Table 9. The ANOVA for the total duration of system trespassing events was statistically significant with an F statistic of 6.14 (p=0.0006). As such, I reject the null hypothesis and conclude that at least one of the means was significantly different for the total duration of the trespassing events. Here, eta-squared indicates that the experimental condition explained about 8.2% of the variation in the total duration of the trespassing events—not as much as the effect size for the number of trespassing events, but a far bigger effect size than found for the average duration of the trespassing event. Next, I utilized post hoc Tukey tests to identify specifically which means were significantly different.

Results for the post hoc Tukey tests for the total duration of system trespassing events are presented in Table 10. To examine whether the type of user affects the total trespassing duration, I compared the conditions by the type of users, while controlling for the number of users. As Table 10 shows, the only significant difference for type of user is between multiple users (administrator) versus multiple users (no administrator). This finding indicates that, for trespassers assigned to target computers with multiple users on them, the presence of an administrative user (compared to a non-administrative user) reduced the total duration of trespassing events by nearly 153 minutes. This reduced the total duration from 214.55 minutes to 61.65 minutes, or from nearly 3.5 hours to 1 hour. This difference, however, was not significant for one user (administrator) compared to one user (no administrator), providing partial support for Hypothesis 1c.

Also indicated in Table 10, holding the type of user constant and comparing across different numbers of users did not result in any significant differences. This conclusion fails to provide support for Hypothesis 2c. However, there was a significant difference when examining across both number and type of users. Trespassers assigned to target computers with multiple users (no administrator) compared to those assigned to one user (administrator) had significantly longer total durations (147 minutes longer). This continues to provide partial support for the importance of the type of user over the number of users in reducing the progression of system trespassing.

Overall, this research provides evidence of support for Hypotheses 1a and 1c, as seen in Table 11. These findings indicate that it is the *type* of user on the system—not the number—that had a significant impact on the number of trespassing events and the total duration of the system trespassing events, but that neither number nor type of users had an effect on the average duration of the system trespassing event.

# Chapter 8: Discussion

This thesis expanded on prior research on system trespassing by investigating the impact of the presence of users on a system on the progression of trespassing events. In general, results indicated that the presence of users on a system did in fact have a significant impact on the progression of trespassing events (though not consistently across all comparisons).

More specifically, this thesis examined whether the number and type of computer users on a system reduced the number of trespassing events, average duration of each event, and total duration of the system trespassing events for system trespassers. Support was found for the presence of an administrative user on a system reducing the number of trespassing events (Hypothesis 1a) and partially for the presence of an administrative user on the system reducing the total duration of trespassing events (Hypothesis 1c). In fact, system trespassers who had target computers with an administrative user present returned to the system between 20 and 22 fewer times than system trespassers who had target computers with only non-administrative users present (reducing the number of trespassing events by about a factor of 5.5) and 14 fewer times than trespassers assigned to target computers with no users present (reducing the number of trespassing events by a factor of 3.5), regardless of the number of users on the system. Additionally, for multiple users on the system, system trespassers with target computers with an administrative user present spent 153 fewer minutes (about 2.5 fewer hours) on the system than trespassers whose target computers did not have an administrative user present, which reduced the total duration by a factor of 3.5. The type of user had no significant effect on the average duration of the trespassing event and the number of users had no significant effects on the number of trespassing events, the average duration of the event, or the total duration of the system trespassing events.

These findings have interesting implications for the application of criminological theories to the cyber world. Generally, this study tested the effect of surveillance or guardianship on the progression of system trespassing. In accordance with SCP and RAT, surveillance and guardianship, respectively, should serve to deter offenders from committing crime. Specifically, this study compared the effects of natural and place manager surveillance. The findings indicate that place manager surveillance (or the presence of an administrative user) may be a more effective deterrent technique in cyberspace than natural surveillance (or controlling the number of users on the system). The lack of significant findings for the number of users on the system indicates that natural surveillance did not play a role in reducing the progression of a trespassing event in this study. In fact, the presence of an administrative user was significant regardless of the total number of users on the system with regards to the number of trespassing events. This indicates that both SCP and RAT are partially supported in this study. The presence of surveillance or a guardian in the form of an administrative user significantly diminished the impact of the crime, by decreasing the number of times a trespasser returned to the system and the total duration of the system trespassing events.

In terms of deterrence, the findings of this study support the hypothesized restrictive deterrent effect, as opposed to an absolute deterrent effect. Although the presence of an administrative user did not significantly reduce the average duration of the event, the significant reduction of the number of trespassing events and total duration of the trespassing events still indicates that the frequency and seriousness of the crime was at least partially reduced.  In other words, trespassers were returning to the system fewer times and, overall, remaining on the system for a shorter duration of time.  Importantly, this indicates that the trespassers may have reduced the number of events, and consequently the amount of time on the system, in an effort to avoid detection, which is evidence of behavior modification consistent with restrictive deterrence.  Additionally, this decrease in the amount of total time on the system results in less opportunity for the trespasser to do damage to the system.

Overall, this research shows support for applying criminological theories to system trespassing.  SCP and RAT are partially supported with regards to place manager surveillance, and the presence of a place manager resulted in the trespasser returning to the system fewer times and spending less total time on the system (resulting in a restrictive deterrent effect).

Policy implications of these findings are fairly straightforward.  IT managers can implement security programs that add the presence of a fake administrative user on the system at all times.  As this thesis suggests, this simple task could reduce the number of times a system trespasser returns to the system and the total amount of time spent on the system, thus reducing the potential damage.  Importantly, the findings presented here do not suggest that the addition of an administrative user would increase the progression of the trespassing event.  However, future research is necessary before this policy can or should be adopted by organizations outside of the university currently evaluated by this thesis, and these results must be taken in light of important limitations.

## ***8.1 Limitations and Future Research***

The limitations of this research are largely due to the data available for analysis. First, these results are questionable in their generalizability beyond the university setting in which this experiment took place. Additionally, there are some limitations in terms of the treatment fidelity of the experiment. As previously mentioned, there is the potential for a single system trespasser to be subject to more than one experimental condition. Because the experiment tracked trespassers based on their IP addresses, those who altered their IP addresses had the potential to regain access to the system on a new target computer and be randomly assigned a different condition. This limitation reduces the assurance of independence of the observations. Yet, if this issue did occur in this data, the same system trespasser experiencing multiple experimental conditions would bias the results toward insignificant findings, which actually strengthens the significance of the findings of this study.

Perhaps one of the most important limitations for this study is the large number of zero observations in the dataset (driven largely by the number of zero event observations). As previously mentioned, the system trespassers who had zeros were not distributed evenly across the experimental conditions. In fact, the two conditions that had administrative users were far more affected by both zero event and zero time observations (i.e. they had a larger proportion of trespassers who had zeros). These zeros are problematic because their uneven distribution could indicate a substantive difference between the trespassing events by system trespassers assigned to target computers with administrative users compared to those assigned to the other conditions. Interestingly, further analysis revealed that the removal of the zeros did not substantially alter the proportion of administrative system trespassers in each condition separately or across conditions altogether. This finding indicates that perhaps the removal of the zeros did not affect the populations of the conditions quite as negatively as expected. However, this sensitivity analysis was limited in scope and only went so far in addressing the potential biasing effect of the nonrandom distribution of zeros. Ultimately, the analysis did not and cannot disprove that there was bias in the uneven distribution of zeros across experimental conditions. Therefore, as it is still difficult to identify the source of the zeros and their unequal distribution, further research is needed to investigate this issue and to guide future research experiments within this domain.

By addressing these limitations, future research can build on this analysis in multiple ways. Implementation of target computer experiments can be incredibly insightful for analyzing the behavior of system trespassers, however it is essential to ensure treatment fidelity and controlled randomization. Future experiments should be executed across different areas, not just on university networks and not just in the United States. Such experiments would provide more rich data regarding system trespasser actions in more generalizable samples. Additionally, future research should investigate other measures of the progression of a trespassing event. Where this study only examined the number of events, average duration of the trespassing event, and total duration of system trespassing events, further research could also explore the commands typed by system trespassers to shed light on the potential deterrent effect of surveillance with regards to the actual actions of the system trespassers while on the system (e.g. whether particular actions are deterred by the surveillance). Moreover, this analysis only looked at the effect of the presence of one administrative user on system trespassing, and future studies should investigate the effects of different numbers of place managers or administrative users. Lastly, future research on the effect of formal surveillance in cyberspace would be germane to investigating the effect of surveillance by allowing for comparison across all three surveillance types.

This work provides further credence to applying criminological theories to system trespassing. However, it is clear that the theories do not work in the cyber world exactly as they do in the physical world; certain theories may only partially apply or may not apply at all. Consequently, this highlights the importance of examining the differences in the mechanisms and outcomes of applying criminological theory to the cyber world versus the physical world.

# Chapter 9: Conclusion

System trespassing is a topical and undesirable phenomenon. As its prevalence increases, so do its deleterious effects to people, companies, and countries. However, research on system trespassing mostly looks at the technical side of the act (i.e. how system trespassers gain access to a system). In terms of the research that does examine system trespassing from a criminological perspective (i.e. the actions of the system trespassers after gaining access to the system), this is the first study examining the effect of the presence of other users on the system on the progression of a system trespassing event. Utilizing ideas of surveillance and restrictive deterrence, this research found that the presence of an administrative user significantly decreased the number of trespassing events and the total duration of the system trespassing events but not the average duration of the trespassing event. This research finds support for the application of SCP (specifically, place manager surveillance), RAT, and restrictive deterrence to the actions of system trespassers, while calling for future research to investigate the promising potential of applying criminological theories to system trespassing.

# Appendices

**Figure 1: Deployment of Target Computers on University Network**

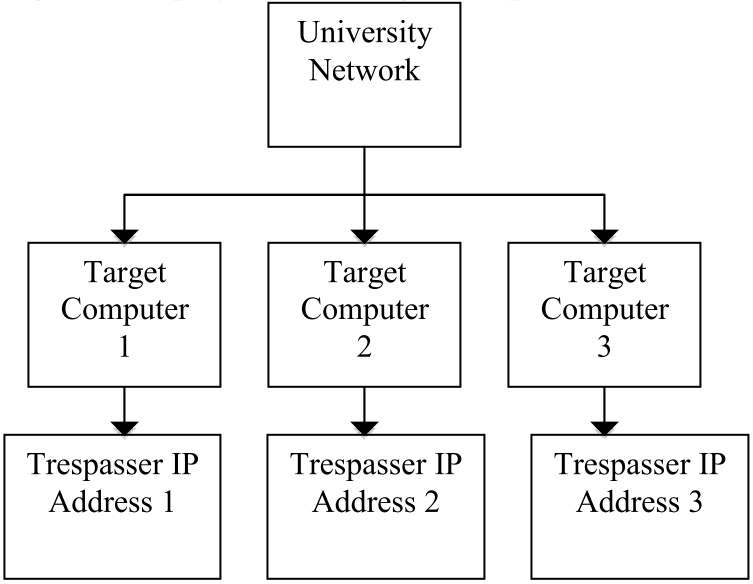

**Figure 2: Process of Infiltrating a Target Computer**

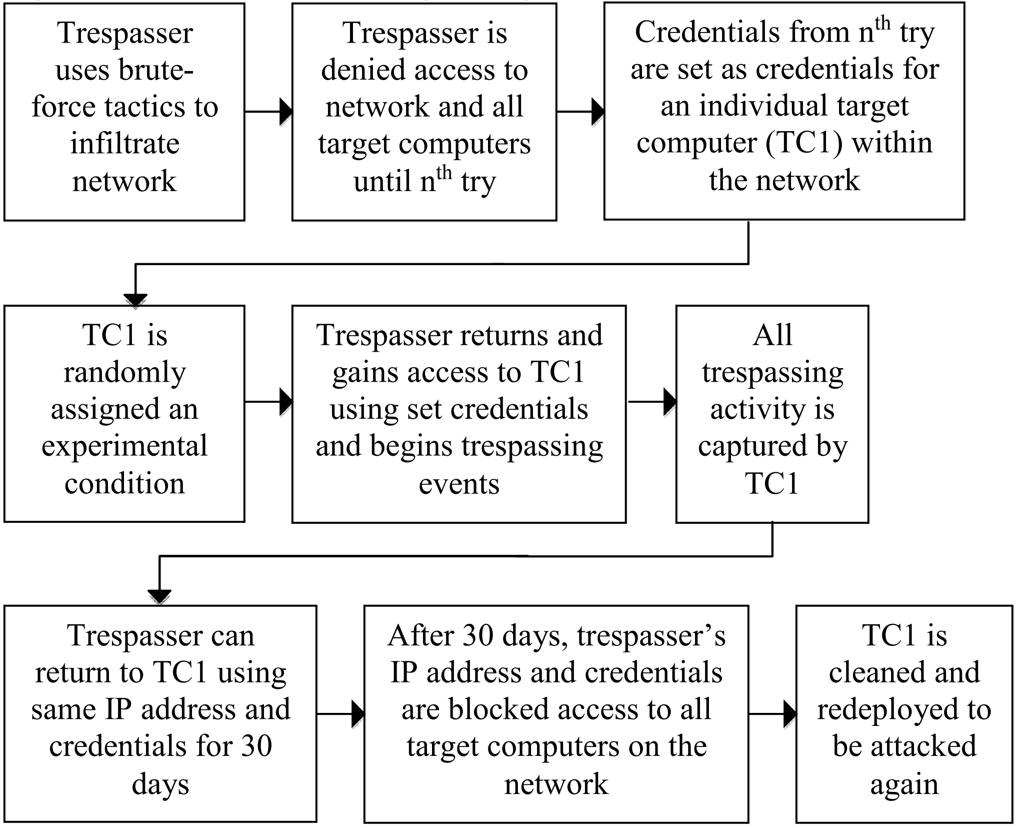
Trespasser uses brute-force tactics to infiltrate network
Trespasser is denied access to network and all target computers until nth try
Credentials from nth try are set as credentials for an individual target computer (TC1) within the network
TC1 is randomly assigned an experimental condition
Trespasser returns and gains access to TC1 using set credentials and begins trespassing events
All trespassing activity is captured by TC1
Trespasser can return to TC1 using same IP address and credentials for 30 days
After 30 days, trespasser's IP address and credentials are blocked access to all target computers on the network
TC1 is cleaned and redeployed to be attacked again

**Figure 3: Histogram of Number of Trespassing Events**

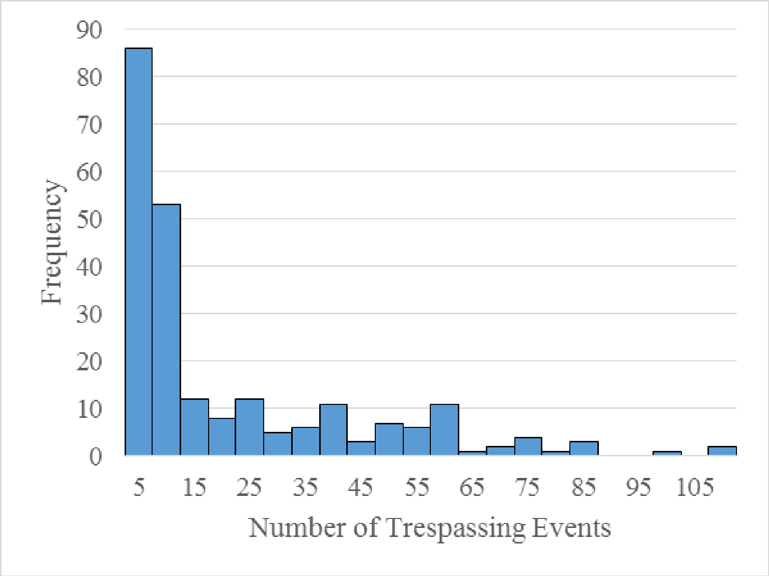

**Figure 4: Histogram of Average Duration of the Trespassing Event**

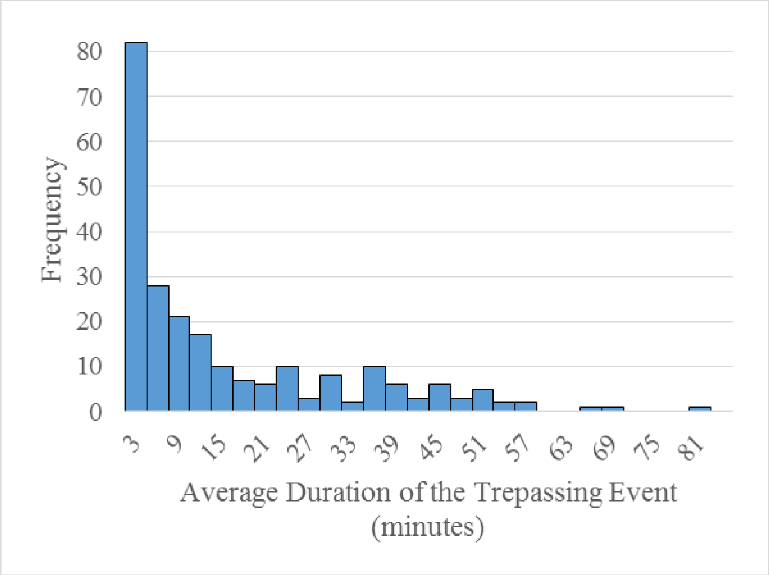

**Figure 5: Histogram of Total Duration of Trespassing Events**

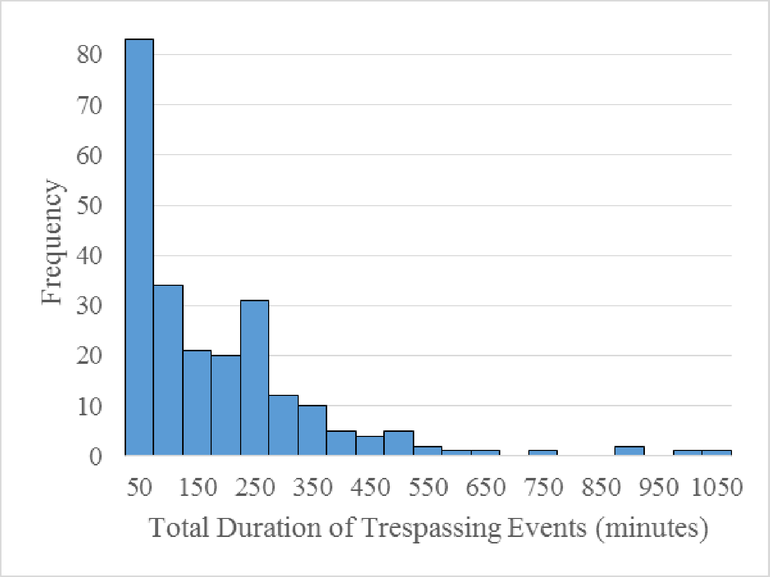

**Table 1: Description of Experimental Conditions**

| | Number of Users | Administrative User Present |
|---|---|---|
| Control | 0 | N |
| One User (No Admin) | 1 | N |
| One User (Admin) | 1 | Y |
| Multiple Users (No Admin) | 10 | N |
| Multiple Users (Admin) | 10 | Y |

**Table 2: Distribution of Zeros in Experimental Conditions**

| | With All Zeros | Without Zero Events | Without Zero Events or Zero Times |
|---|---|---|---|
| Control | 90 | 68 | 66 |
| One User (No Admin) | 93 | 69 | 68 |
| One User (Admin) | 91 | 28 | 24 |
| Multiple Users (No Admin) | 84 | 61 | 60 |
| Multiple Users (Admin) | 90 | 25 | 21 |
| Total | 448 | 251 | 239 |

**Table 3: Distribution of Administrative System Trespassers**

| | Control | One User (No Admin) | One User (Admin) | Multiple Users (No Admin) | Multiple Users (Admin) | Total |
|---|---|---|---|---|---|---|
| With All Zeros | | | | | | |
| Non-Admin | 11<br>(12.22%) | 10<br>(10.75%) | 10<br>(10.99%) | 13<br>(15.48%) | 11<br>(12.22%) | 55<br>(12.28%) |
| Admin | 79<br>(87.78%) | 83<br>(89.25%) | 81<br>(89.01%) | 71<br>(84.52%) | 79<br>(87.78%) | 393<br>(87.72%) |
| Without Zeros | | | | | | |
| Non-Amin | 4<br>(6.06%) | 1<br>(1.47%) | 2<br>(8.33%) | 3<br>(5.00%) | 2<br>(9.52%) | 12<br>(5.02%) |
| Admin | 62<br>(93.94%) | 67<br>(98.53%) | 22<br>(91.67%) | 57<br>(95.00%) | 19<br>(90.48%) | 227<br>(94.98%) |

**Table 4: Descriptive Statistics of Dependent Variables (n=234)**

| | Mean | Median | Min | Max |
|---|---|---|---|---|
| Number of Trespassing Events | 19.30 | 8 | 1 | 108 |
| Average Event Duration (minutes) | 13.83 | 6.79 | .01 | 78.61 |
| Total Duration of Events (minutes) | 151.94 | 100.13 | .02 | 1021.88 |

**Table 5: Descriptive Statistics by Experimental Condition**

| | Number of Trespassers | Total Number of Trespassing Events | Average Number of Trespassing Events Per Trespasser | Average Mean Event Duration Per Trespasser | Average Total Duration of Events Per Trespasser |
|---|---|---|---|---|---|
| Control | 65 | 1201 | 18.48 | 13.42 | 146.42 |
| One User (No Admin) | 67 | 1596 | 23.82 | 10.62 | 162.72 |
| One User (Admin) | 24 | 104 | 4.33 | 19.02 | 67.06 |
| Multiple Users (No Admin) | 57 | 1523 | 26.72 | 15.39 | 214.55 |
| Multiple Users (Admin) | 21 | 93 | 4.43 | 15.20 | 61.65 |

**Table 6: ANOVA for Number of Trespassing Events**

| | SS | df | MS | F | Prob > F | Eta Sq |
|---|---|---|---|---|---|---|
| Between groups | 14571.41 | 4 | 3642.85 | 7.70 | 0.0000 | 0.119 |
| Within groups | 108308.05 | 229 | 472.96 | | | |
| Total | 122879.46 | 233 | 527.38 | | | |

**Table 7: Post Hoc Tukey Tests for Number of Trespassing Events**

| | Contrast | t |
|---|---|---|
| One User (No Admin) vs. Control | 5.34<br>(3.79) | 1.41 |
| One User (Admin) vs. Control | -14.14<br>(5.19) | -2.72* |
| Multiple Users (No Admin) vs. Control | 8.24<br>(3.95) | 2.09 |
| Multiple Users (Admin) vs. Control | -14.05<br>(5.46) | -2.57* |
| One User (Admin) vs. One User (No Admin) | -19.49<br>(5.17) | -3.77** |
| Multiple Users (No Admin) vs. One User (No Admin) | 2.90<br>(3.92) | 0.74 |
| Multiple Users (Admin) vs. One User (No Admin) | -19.39<br>(5.44) | -3.57** |
| Multiple Users (No Admin) vs. One User (Admin) | 22.39<br>(5.29) | 4.23** |
| Multiple Users (Admin) vs. One User (Admin) | -0.10<br>(6.50) | 0.01 |
| Multiple Users (Admin) vs. Multiple Users (No Admin) | -22.29<br>(5.55) | -4.02** |

Note: Standard errors are shown in parentheses.
* p<.05 one-tailed
** p<.01 one-tailed

**Table 8: ANOVA for Average Duration of Event**

| | SS | df | MS | F | Prob > F | Eta Sq |
|---|---|---|---|---|---|---|
| Between groups | 1524.06 | 4 | 381.02 | 1.47 | 0.2122 | 0.025 |
| Within groups | 59367.70 | 229 | 259.25 | | | |
| Total | 60891.76 | 233 | 261.34 | | | |

**Table 9: ANOVA for Total Duration of Trespassing Events**

| | SS | df | MS | F | Prob > F | Eta Sq |
|---|---|---|---|---|---|---|
| Between groups | 577335.88 | 4 | 144333.97 | 6.14 | 0.0006 | 0.082 |
| Within groups | 6435846.59 | 229 | 28104.13 | | | |
| Total | 7013182.47 | 233 | 30099.50 | | | |

**Table 10: Post Hoc Tukey Tests for Total Duration of Trespassing Events**

| | Contrast | t |
|---|---|---|
| One User (No Admin) vs. Control | 16.30<br>(29.19) | 0.56 |
| One User (Admin) vs. Control | -79.36<br>(40.04) | -1.98 |
| Multiple Users (No Admin) vs. Control | 68.13<br>(30.42) | 2.24 |
| Multiple Users (Admin) vs. Control | -84.77<br>(42.08) | -2.01 |
| One User (Admin) vs. One User (No Admin) | -95.66<br>(39.88) | -2.40 |
| Multiple Users (No Admin) vs. One User (No Admin) | 51.84<br>(30.21) | 1.72 |
| Multiple Users (Admin) vs. One User (No Admin) | -101.07<br>(41.93) | -2.41 |
| Multiple Users (No Admin) vs. One User (Admin) | 147.49<br>(40.79) | 3.62** |
| Multiple Users (Admin) vs. One User (Admin) | -5.41<br>(50.09) | -0.11 |
| Multiple Users (Admin) vs. Multiple Users (No Admin) | -152.90<br>(42.79) | -3.57** |

Note: Standard errors are shown in parentheses.
** p<.01 one-tailed

**Table 11: Conclusions of Hypotheses**

| | Conclusion |
|---|---|
| Administrative Users (Place Manager Surveillance) | |
| Number of Events (1a) | + |
| Average Duration of Each Event (1b) | - |
| Total Duration of System Trespassing Events (1c) | +/- |
| Number of Users (Natural Surveillance) | |
| Number of Events (2a) | - |
| Average Duration of Each Event (2b) | - |
| Total Duration of System Trespassing Events (2c) | - |

+ Supported
+/- Partially Supported
- Not Supported

# Glossary

Brute-Force Entry: Using an automated method to attempt large quantities of username and password combinations in order to illegally gain access to a system

IP Address: Unique public identification numbers assigned to every computer

Network: A group of computer systems that are linked together through communication channels

System Trespassing: Unlawfully gaining access to a computer system

Target Computer: Virtual or physical host used to collect activity of system trespassers

Trespasser (i.e. System Trespasser): Individual who unlawfully gains access to a computer system

Trespassing Event (i.e. Trespassing Incident): Time of communication between the trespasser's system and the infiltrated system

# Bibliography

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace.* ABC-CLIO.

Brumfield, G. (1999). Security systems protective measures against hackers. *General Practice, Solo & Small Firm Division Magazine*.

Bureau of Justice Statistics. (2005). *National computer security survey*. Retrieved from http://www.bjs.gov/index.cfm?ty=tp&tid=41

Christensson, P. (2011). *Session Definition.* Retrieved from http://techterms.com

Clarke, R. V. (1980). "Situational" crime prevention: Theory and practice. *The British Journal of Criminology*, 136-147.

Clarke, R. V. (1995). Situational crime prevention. *Crime and justice*, 91-150.

Clarke, R. V. (1997). *Situational crime prevention: Successful case studies.* Albany, NY: Harrow and Heston.

Clarke, R. V., & Cornish, D. B. (1985). Modeling offenders' decisions: A framework for research and policy. *Crime and justice*, 147-185.

Clarke, R. V., & Homel, R. (1997). A revised classification of situational crime prevention techniques. In S. Lab (ed.), *Crime prevention at a crossroads.* Cincinnati, OH: Anderson Publishing Company.

Cornish, D. B., & Clarke, R. V. (1986). *The reasoning criminal*. New York: Springer-Verlag.

Cornish, D. B., & Clarke, R. V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies, 16*, 41-96.

Cukier, M., Maimon, D., & Berthier, R. (2012, July). A journey towards rigorous cybersecurity experiments: On the application of criminological theories. In *Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results* (pp. 25-30). ACM.

Eck, J. (1997). *Preventing crime at places*. National Institute of Justice. Retrieved from https://www.ncjrs.gov/works/

Erickson, H., & Houck, J. (2005). *CPTED security: Crime prevention through environmental design*. Retrieved from http://cptedsecurity.com/cpted_design_guidelines.htm

Esterbrook, J. (2002). *Many hack attacks go unreported.* Retrieved from http://www.cbsnews.com/news/many-hack-attacks-go-unreported/

Evans, M. (2015, February 15). *Hackers steal £650 million in world's biggest bank raid*. Retrieved from http://www.telegraph.co.uk/news/uknews/crime/11414191/Hackers-steal-650-million-in-worlds-biggest-bank-raid.html

Exum, M. L., Kuhns, J. B., Koch, B., & Johnson, C. (2010). An examination of situational crime prevention strategies across convenience stores and fast-food restaurants. *Criminal Justice Policy Review*, *21*(3), 269-295.

Farhat, V., McCarthy, B., & Raysman, R. (2011). *Cyber attacks: Prevention and proactive responses* (1st ed., pp. 1-12). Practical Law Company.

Felson, M. (1995). Those who discourage crime. *Crime and Place, 4*, 53-66.

Friedman, G. (2015, September 30). *FBI releases inaugural hacking stats*. Retrieved from https://bol.bna.com/fbi-releases-inaugural-hacking-stats/

Graham, K. (2009). They fight because we let them! Applying a situational crime prevention model to barroom violence. *Drug and Alcohol Review*, *28*(2), 103-109.

Gibbs, J. (1975). *Crime, punishment, and deterrence*. New York: Elsevier.

Hayes, R., Downs, D. M., & Blackwood, R. (2012). Anti-theft procedures and fixtures: A randomized controlled trial of two situational crime prevention measures. *Journal of Experimental Criminology*, *8*(1), 1-15.

Hollis-Peel, M. E., Reynald, D. M., van Bavel, M., Elffers, H., & Welsh, B. C. (2011). Guardianship for crime prevention: A critical review of the literature. *Crime, law and social change*, *56*(1), 53-70.

Homeland Security. (2015). *Securing federal networks*. Retrieved from http://www.dhs.gov/topic/securing-federal-networks#

Huey, L., & Rosenberg, R. S. (2004). Watching the web: Thoughts on expanding police surveillance opportunities under the cyber-crime convention. *Canadian Journal of Criminology & Criminal Justice, 46*(5), 597-606.

Huisman, W., & van Erp, J. (2013). Opportunities for environmental crime: A test of situational crime prevention theory. *British journal of criminology*, *53*(6), 1178-1200.

Jacobs, B. A. (2010). Deterrence and deterrability. *Criminology, 48*, 417-441.

Kim, W., Jeong, O. R., Kim, C., & So, J. (2011). The dark side of the Internet: Attacks, costs and responses. *Information Systems*, *3*(36), 675-705.

Madensen, T. D., & Eck, J. E. (2008). Violence in bars: Exploring the impact of place manager decision-making. *Crime Prevention and Community Safety, 10*(2), 111-125.

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

Maimon, D., Kamerdze, A., Cukier, M., & Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network: An application of the routine-activities and lifestyle perspective. *British journal of criminology*, *53*(2), 319-343.

Maimon, D., Wilson, T., Ren, W., & Berenblum, T. (2015). On the relevance of spatial and temporal dimensions in assessing computer susceptibility to system trespassing incidents. *British Journal of Criminology*, *55*(3), 615-634.

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

Mickelberg, K., Pollard, N., & Shive, L. (2014). *US cybercrime: Rising risks, reduced readiness* (pp. 1-19). Pricewaterhouse Coopers.

Moon, P. (2015). *Ashley Madison hack reveals the lies and deceptions we have come to accept online*. Retrieved from http://www.afr.com/technology/ashley-madison-hack-reveals-the-lies-and-deceptions-we-have-come-to-accept-online-20150821-gj4vxy

Moore, A. D. (2000). Employee monitoring and computer technology: Evaluative surveillance v. privacy. *Business Ethics Quarterly, 10*(3), 697-709.

Mueller, M., & Kuehn, A. (2013). Einstein on the breach: Surveillance technology, cybersecurity and organizational change. In *12th Workshop on the Economics of Information Security (WEIS 2013), Georgetown University, Washington, DC June* (pp. 11-12).

Painter, K. A., & Farrington, D. P. (2001). Evaluating situational crime prevention using a young people's survey: Part ii making sense of the elite police voice. *British Journal of Criminology*, *41*(2), 266-284.

Ponemon Institute. (2015). *2015 Cost of Cyber Crime Study* (pp. 1-29).

Pratt, T. C., Holtfreter, K., & 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*(3), 267-296.

Rubens, P. (2015). *Cybersecurity: Defending 'unpreventable' cyber attacks*. Retrieved from http://www.bbc.com/news/business-31048811

Shane, J. M., Piza, E. L., & Mandala, M. (2015). Situational crime prevention and worldwide piracy: A cross-continent analysis. *Crime Science*, *4*(1), 1-13.

Spitzner, L. (2003). *Honeypots: Tracking hackers*. Boston, MA: Pearson Education, Inc.

Stallings, W. (2005). *Wireless communications and networks.* Pearson Prentice Hall.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255-276.

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

von Lampe, K. (2011). The application of the framework of situational crime prevention to ‘organized crime’. *Criminology and Criminal Justice*, *11*(2), 145-163.

Wall, D. S. (Ed.). (2003). *Crime and the Internet*. Routledge.

Wall, D. S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers and Technology*, *22*(1-2), 45-63.

Weenink, A. W. (2012). Situational prevention of terrorism. Remarks from the field of counterterrorism in the Netherlands on Newman and Clarke’s Policing Terrorism. *Trends in Organized Crime*, *15*(2-3), 164-179.

Welsh, B. C., & Farrington, D. P. (2004). Surveillance for crime prevention in public space: Results and policy choices in Britain and America. *Criminology & Public Policy, 3*(3), 497-526.

Welsh, B. C., & Farrington, D. P. (2009). Public area CCTV and crime prevention: An updated systematic review and meta-analysis. *Justice Quarterly, 26*(4), 716-745.

Wilcox, P., Madensen, T. D., & Tillyer, M. S. (2007). Guardianship in context: Implications for burglary victimization risk and prevention. *Criminology, 45*(4), 771-803.

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