University of South Florida
Scholar Commons

Graduate Theses and Dissertations

Graduate School

6-13-2016

The Restrictive Deterrent Effect of Warning Banners in a Compromised Computer System

Christian Jordan-Michael Howell
University of South Florida, cjhowell@mail.usf.edu

Follow this and additional works at: http://scholarcommons.usf.edu/etd

Part of the Criminology and Criminal Justice Commons

Scholar Commons Citation

Howell, Christian Jordan-Michael, "The Restrictive Deterrent Effect of Warning Banners in a Compromised Computer System" (2016). *Graduate Theses and Dissertations.*
http://scholarcommons.usf.edu/etd/6259

This Thesis is brought to you for free and open access by the Graduate School at Scholar Commons. It has been accepted for inclusion in Graduate Theses and Dissertations by an authorized administrator of Scholar Commons. For more information, please contact scholarcommons@usf.edu.

The Restrictive Deterrent Effect of Warning Banners in a Compromised Computer System

by

Christian Jordan-Michael Howell

A thesis submitted in partial fulfillment
of the requirements for the degree of
Master of Arts
Department of Criminology
College of Behavioral and Community Sciences
University of South Florida

Co-Major Professor: John Cochran, Ph.D.
Co-Major Professor: David Maimon, Ph.D.
Ráchael Powers, Ph.D.

Date of Approval:
June 13, 2016

Keywords: Cybercrime, Particularistic restrictive deterrence, Hacking, Hackers, System trespassers

Copyright © 2016, Christian Jordan-Michael Howell

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

System trespassing, which refers to the unauthorized access of computer systems, has rapidly become a worldwide phenomenon. Despite growing concern, criminological literature has paid system trespassing little attention. The current study utilizes data gathered from a Chinese computer network to examine system trespasser behavior after exposure to one of three warning messages: an altruistic message used for moral persuasion (warning 1), a legal sanction threat (warning 2), and an ambiguous threat (warning 3). More specifically, the current study examines the temporal order of various keystroke commands to determine if some keystroke commands are used as a tactical skill to avoid detection. The results of a series of bivariate cross-tabulations show that encountering a standard legal threat or ambiguous threat increase the early use of reconnaissance commands; however, these findings were not pronounced enough to gain statistical significance. Since the current study is the first known test of particularistic restrictive deterrence in cyberspace it informs those working in cyber security, whilst expanding the scope of the theory.

Introduction

System trespassing, the unauthorized access of computer systems, has rapidly become a worldwide phenomenon with an estimated annual cost to the global economy of over $400 billion (McAfee, 2014). The average cost of system trespassing to United States companies in 2015 has been estimated at roughly $15 million (Ponemon Institute, 2013). Additionally, at the individual level, system trespassers (also known as hackers) can gain access to sensitive information, which can be used to fuel identity theft or even to invade one's personal privacy. Despite growing concern, the criminological literature has paid system trespassing little attention, until Maimon and colleagues' (2014) study. Maimon and colleagues (2014) tested the restrictive deterrent effect (i.e., efforts by active offenders to reduce their odds of getting caught and punished) of warning banners on post-compromised target computers (also known as honeypots). Maimon and colleagues (2014) employed honeypot computers built for the purpose of being attacked, and conducted two experiments to examine the influence of warning banners on the progression, frequency, and duration of system trespassing incidents. They found that a warning banner significantly increases the rate of first system trespassing termination, and decreases the duration of first trespassing incidents.

Due to the success of Maimon and colleagues' (2014) study, the deterrent effect of warning banners has gained an increasing amount of criminological attention (Jones, 2014; Wilson, Maimon, Sobesto, & Cukier, 2015). Although subsequent studies have made significant advancements in the current body of literature, additional research is imperative to gain a fuller understanding of the restrictive deterrent effects of warning banners on system trespasser behavior. Particular attention should be paid to the existence of particularistic restrictive deterrence in cyberspace. Particularistic restrictive deterrence is the modification of behavior based on “tactical skills offenders use that make them less likely to be apprehended” (Jacobs, 1996a, p. 425). To date there is no known study of particularistic restrictive deterrence in cyberspace, despite its relevance in the physical world.

Building upon the work of Maimon and colleagues (2014) and Jones (2014), the current study seeks to address this need by examining the temporal order of keystroke commands logged by system trespassers during an intrusion. Examining the temporal order of specific keystroke commands in relation to the treatment or control conditions allows us to examine the extent to which system trespassers modify their behavior after they encounter various warning messages.

Literature Review

Theoretical Background

Paternoster (2010) conceptualized deterrence as the omission of a criminal act due to the fear of punishment. The concept of deterrence, as defined by Paternoster (2010), originated from the work of Cesare Beccaria and Jeremy Bentham. Becarria's classic work, *On Crimes and Punishment,* was written in 1764 in an effort to challenge the rights of the state to punish crime. Beccaria (1963 [1764]) described man as rational and self-interested, thus arguing that one will not commit crime if the cost of committing crime is greater than the benefit. Becarria (1963 [1764]) contended that swift and certain punishment are the best forms of crime prevention, and stated that if punishment is solely to prevent crime then punishment is unjust when its severity exceeds that necessary to deter. Similarly, Bentham (1948 [1789]) believed that the duty of the state was to promote societal happiness, by punishing and rewarding. Like Becarria (1963 [1764]), Bentham (1948 [1789]) believed in proportionality, deeming punishment that exceeds that necessary to deter as unjust.

The early work of Becarria (1963 [1764]) and Bentham (1948 [1789]) became the foundation for deterrence theory and classical criminology. However, in spite of a seemingly well-developed theory explaining criminal behavior, criminologists shifted to a biological positivist approach derived from works such as *Darwin's On the Origin of Species* (Paternoster, 2010). Criminological distaste for deterrence theory was well documented with critiques such as that offered by Von Hentig (1938). Von Hentig (1938) deemed deterrence theory as unreal and simple-minded, stating that a large group of persons cannot be deterred by threats of law. He later argued that deterrence is destined to fail because the pleasure of committing a criminal act is a near object, whereas the cost associated is a long distance danger (Von Hentig, 1938). Similarly, other prominent criminologists dismissed deterrence as a viable crime control model on the grounds that punishment is an ineffective way to change one's behavior (Appel & Peterson, 1965; Toby, 1964).

Deterrence theory came close to being discredited by the scientific community until two studies appeared in 1968 and revitalized criminological interest (Paternoster, 2010). The first was Gary Becker's (1968) study, which took an economic approach to explaining criminal behavior as an act of rational self-interest that can be understood like any other economic activity. Becker (1968) argued that an offender's decision to offend is made up of weighing the costs and benefits of committing a crime in comparison to not committing a crime. Second was Gibbs' (1968) study, which exclusively focused on the effects of punishment on criminal behavior. More importantly, Gibbs (1968) provided an example of how to empirically test deterrence theory by examining the relationship between the certainty and severity of punishments across individual states.

The work of Becker (1968) and Gibbs (1968) paved the way for contemporary criminologists to provide subsequent empirical testing and a more in-depth consideration of deterrence theory. The former led to the development of micro-social analyses of offender decision-making, which in turn has become the study of perceptual deterrence (Paternoster, 2010). The latter led to the development of macro-social studies of deterrence and rates of crime (Paternoster, 2010). Additional advancements include the work of Zimring and Hawkins (1973) and Gibbs (1975), who further differentiated between general and specific deterrence. General deterrence, as conceptualized by Gibbs (1975), refers to the effects of the threat of legal sanctions on the general public, whereas specific deterrence refers to the effects of legal sanctions on those who have suffered it. Furthermore, Gibbs (1975) recognized that legal sanctions can deter crime in various ways. For example, some individuals refrain from all forms of unlawful acts to avoid punishment. Gibbs (1975) referred to such cases as absolute deterrence. Paternoster (1989) differentiated between two types of absolute deterrence. First, there is absolute deterrence when those who have never committed the offense in question continue to refrain due to their fear of sanctions. Second, there is absolute deterrence when those who have committed the offense in question subsequently refrain from continued participation due to their fear of sanctions.

In other instances the threat of legal sanctions do not cause individuals to abstain fully from crime, but instead curtail or modify their criminal behavior to reduce the risk of punishment. Gibbs (1975) referred to such cases as restrictive deterrence. Moreover, restrictive deterrence only applies to those who have committed the crime in question at least once, thus deeming it a function of specific deterrence (Gibbs, 1975). In attempt to conceptually refine restrictive deterrence, Paternoster (1989) contended that restrictive deterrence is a direct reference to the frequency of subgroup offending. In other words, “restrictive deterrence can only be observed for those who, during a given measurement period, have made the participation decision” (Paternoster, 1989, p. 290). Simply put, restrictive deterrence only applies to those who actively engage in the offense in question. Therefore, in accordance to Gibbs (1975) and Paternoster (1989), restrictive deterrence is the curtailment or modification of criminal behavior aimed to reduce the risk of sanctions for those who make the decision to participate in a particular offense. Examples include drug dealers who limit their customer base to avoid selling to undercover police officers (Jacobs, 1996a) and auto thieves who employ tactical skills to evade detection (Jacobs & Cherbonneau, 2014). These, along with other examples of offenders reducing and modifying their behavior to avoid sanctions, are discussed in more depth below.

Paternoster (1989) examined the restrictive deterrent effects on a panel of high school students' perceptions of punishment severity and perceived certainty on four minor delinquent offenses. Paternoster (1989) failed to find a restrictive deterrent effect for the perceived severity of punishment. However, he did find that perceived certainty of punishment has a restrictive deterrent effect, which is particularly strong for marijuana use (Paternoster, 1989). In other words, Paternoster (1989) found that high school students curtail their offense frequency rather than fully abstain from committing the illicit act when they believe that they will be sanctioned. These preliminary findings suggested the utility of differentiating between absolute and restrictive deterrence.

Jacobs (1996a) further expanded upon Paternoster's (1989) conceptual refinement with his ethnographic study of crack dealers. More specifically, Jacobs (1996a) identified, and found support for, two distinct types of restrictive deterrence: probabilistic and particularistic. Probabilistic restrictive deterrence refers to that suggested by Gibbs (1975), which is a curtailment in offense frequency based on an odds, or law of averages mentality (Jacobs, 1996a). In other words, offenders commit less crime in hopes that it will decrease their probability of getting caught. Particularistic restrictive deterrence however, refers to the modification of behavior based on "tactical skills offenders use that make them less likely to be apprehended" (Jacobs, 1996a, p. 425). Tactical skills vary by offense, but are developed as a mechanism to avoid punishment. Moreover, in contrast to Gibbs (1975), Jacobs (1996a) contended that restrictive deterrence could be a function of either specific or general deterrence, or in some cases both simultaneously. More specifically, restrictive deterrence has a specific deterrent effect when one has been previously sanctioned, a general deterrent effect when one has heard others have been sanctioned, and an interaction effect between the two when both instances have occurred (Jacobs, 1996a). Therefore, in essence, both specific and general deterrence can affect all people through the experience of punishment, and it is common that both types affect the same person (Jacobs, 1996a).

Direct empirical examinations of restrictive deterrence are relatively scarce (Gallupe, Bouchard, & Caulkins, 2011; Jacobs, 1993, 1996a, 1996b; Jacobs & Cherbonneau, 2014; Jacobs & Miller, 1998; Paternoster, 1989), qualitative in nature (Jacobs, 1993, 1996a, 1996b; Jacobs & Cherbonneau, 2014), and reliant on small samples (Jacobs, 1996b; Jacobs & Cherbonneau, 2014). Despite these limitations, the aforementioned studies have played an important role in our understanding of how offenders attempt to reduce their risk of sanctions.

For example, Jacobs and Cherbonneau (2014) found support for particularistic restrictive deterrence, in that auto thieves reduce their risk of punishment in three ways: discretionary target selection, normalcy illusions, and defiance. Simply put, discretionary target selection is choosing to steal a car that will not be as easily recognizable. This technique aligns with past target hardening research, in that offenders chose easier targets (Cromwell & Olson, 2004; Rengert & Wasilchick, 1989; Wright & Decker, 1994, 1997). The normalcy illusion involves using specific tactics to keep authorities, victims, and witnesses from becoming wise (Goffman, 1963). Defiance refers to the rejection of sanction threats (Jacobs & Cherbonneau, 2014). In other words, defiance is the avoidance of apprehension by fleeing the scene once caught. These techniques exemplify the ways in which punishment is avoided at all stages of the auto burglary process. Auto thieves employ discretionary target selection when deciding which car to steal.

Once they have successfully stolen a car they elude police detection with the normalcy illusion. If the above techniques fail, the auto thief is defiant and ready to flee the scene.

Jacobs (1993) examined perceptual shorthands dealers use to determine whether buyers in question are undercover police officers. He found two commonly used perceptual shorthands, which he later refers to as tactical skills (Jacobs, 1996a): trend discontinuity and interpersonal illegitimacy. Trend discontinuity is when familiar customers introduce unfamiliar others who desire to buy drugs, and when familiar customers suddenly and significantly increase the quantities in which they wish to purchase (Jacobs, 1993). Dealers become skeptical and begin worrying that the familiar buyer has become a police informant. Interpersonal illegitimacy is when unfamiliar buyers radiate certain vibes believed to be indicative of an undercover agent (Jacobs, 1993). Jacobs and Miller (1998) found that female crack dealers avoid detection in a similar manner, yet are typically much more discrete. Although being discrete makes it harder for police to detect a female dealer, it also limits their customer base.

Gallupe and colleagues (2011) applied the concept of restrictive deterrence to a sample of drug market offenders. More specifically, they assessed the influence of behavioral changes post-arrest on time to re-arrest (Gallupe, Bouchard, & Caulkins, 2011). They found that switching location is correlated to more rapid re-arrest, unless dealing with cannabis cultivation, in which changing location leads to a longer period before re-arrest (Gallupe, Bouchard, & Caulkins, 2011).

Although direct empirical examinations of restrictive deterrence are still relatively scarce, there is a large body of literature that indirectly examines the concept of restrictive deterrence under situational crime prevention and routine activity theory. Situational crime prevention, as defined by Clarke (1997), is " (1) directed at highly specific forms of crime, (2) involves the management, design, or manipulation of the immediate environment in as systematic and permanent way as possible, (3) makes crime more difficult and risky, or less rewarding and excusable as judged by a wide range of offenders" (p. 4). Clark (1997) continues by listing a plethora of successful situational crime prevention measures aimed to curtail criminal behavior:

> surveillance cameras for subway systems and parking facilities, defensible space architecture in public housing, target hardening of apartment blocks and individual residences, electronic access for cars and for telephone systems, street closures and traffic schemes for residential neighborhoods, alcohol controls at festivals and sporting fixtures, training in conflict management for publicans and bouncers, and improved stocktaking and record keeping procedures in warehouse and retail outlets. (p.3)

Moreover, Clark (1997) contends that it is common for the average person to routinely utilize situational crime prevention measures to avoid being victimized such as locking the door, securing valuables, buying houses in safe neighborhoods, investing in burglar alarms, and avoiding dangerous people and places.

Situational crime prevention dates back to the 1960s and 1970s with work on correctional treatments conducted by the Home Office Research Unit, the British government's criminological research department (Clarke & Cornish, 1983). Arguably most influential was the finding that school children misbehave based on their opportunity to do so rather than their personality or background; therefore, Tizard and colleagues (1975) thought it possible to design out misbehavior.

Support for the Home Office position was found in criminological literature on property offending (Burt, 1925), childhood dishonest behavior (Hartshorne & May, 1928), and geographical studies on auto burglary (Wilkins, 1964). The Home Office position also paralleled contemporary psychological research. Examples include the work of Mischel (1968), who found that situational influences played a greater role in shaping individual behavior than previously thought, and Matza (1964) who contended that individuals drift into deviancy rather than adhere to a strong deviant bond.

Tedeschi and Felson (1994) extended situational crime prevention measures to even the most serious of crimes. For example, they found that homicide is influenced by availability of handguns (Tedeschi & Felson, 1994). Similarly, Wilkinson (1986) accredited the virtual elimination of aircraft hijackings to increased baggage screening, and Gabor (1990) and Grandjean (1990) accredited the reduction in bank robberies to target hardening techniques, such as bulletproof glass windows.

At the same time situational crime prevention was gaining momentum in Britain, scholars in the United States were developing similar concepts such as defensible space (Newman, 1972) and crime prevention through environmental design or CPTED (Jeffery, 1971). Newman (1972) provided empirical support linking large-scale public housing buildings to increased crime rates. He argued that the design of public housing makes it impossible to know your neighbors, which discourages residents from exercising their normal territorial instincts to exclude offenders (Newman, 1972). Similarly, Jeffery's CPTED drew from the biosocial theory of learning and "argued that punishment and treatment philosophies had to be abandoned in favor of a preventive approach which took due account of both genetic predisposition and the physical environment" (Clarke, 1997, p. 8).

In addition to CPTED and situational crime prevention, restrictive deterrence draws support from routine activity theory. Routine activity theory states that three elements must be present for a crime to occur: a likely offender, a suitable target, and the absence of a capable guardian (Cohen & Felson, 1979). Paralleling the literature on restrictive deterrence, Cohen and Felson (1979) found that the shift to a greater participation of women in the workforce led to an increase in burglaries due to the greater proportion of empty houses. In other words, the increase in burglaries can be accredited to the decrease in restrictive deterrence that resulted from burglars' decreased fear of sanctions.

Further advancements in deterrence literature suggest that for the deterrence process to be successful, warning messages must be displayed to the target audience (Geerken & Gove, 1975). A large body of literature has examined the effectiveness of warning offenders of possible sanctions, but found mixed results (Coleman, 2007; Decker, 1972; Eck & Wartell, 1998; Grabosky, 1996; Lowman, 1992; Rama & Kulmala, 2000). For example, warning banners have no effect on prostitution (Loman, 1992), yet decrease unsafe driving (Rama & Kulmala, 2000), tax evasion (Coleman, 2007) and open drug dealing (Eck & Wartell, 1998). Interestingly, warning banners have an adverse effect on petty crimes such as pickpocketing (Grabosky, 1996). For these petty crimes, Grabosky (1996) suggested that waning banners act as advertisement, thus encouraging illicit behavior. The present study seeks to extend these empirical examinations to cyberspace.

Deterrence in Cyberspace

Although an immense body of restrictive deterrence literature has accumulated, criminologists have failed to examine its relevance in cyberspace, until Maimon and colleagues' (2014) study. Maimon and colleagues (2014) employed target computers on a large American university and conducted two independent experiments to examine the influence of a single warning banner on the progression, frequency, and duration of system trespassing incidents. The target computers in both experiments were programed to exhibit or not to exhibit a warning banner once hackers had successfully infiltrated the systems. Maimon and colleagues (2014) found that a warning banner significantly increases the rate of first system trespassing termination, and decreases the duration of first trespassing incidents. The findings emphasized the relevance of restrictive deterrence in cyberspace, which were later corroborated by research in information technology (Stockman, Heile, & Rein, 2015).

Due to the success of Maimon and colleagues' (2014) study, the deterrent effect of warning banners has gained an increasing amount of criminological attention (Jones, 2014; Wilson, Maimon, Sobesto, & Cukier, 2015). For example, Jones (2014) examined system trespassers' behavior using a non-American computer network. Similar to Maimon and colleagues (2014), the target computers used in Jones' (2014) study were programed to exhibit or not to exhibit a warning banner once hackers had successfully infiltrated the systems. Unlike the Maimon and colleagues (2014) study, Jones (2014) utilized three warning banners: an altruistic message used for moral persuasion (warning 1), a legal sanction threat (warning 2), and an ambiguous threat (warning 3). In doing this, Jones (2014) was able to look beyond the frequency and duration of a system trespass, and instead examine the effects of different warning banners on individual keystrokes. Interestingly, Jones (2014) found that the altruistic message had a deterrent effect; whereas the legal sanction threat and ambiguous threat increased command usage.

Wilson and colleagues (2015) examined whether the presence of a surveillance banner on a compromised computer system influenced attackers' engagement with the compromised system. A compromised computer system is a computer that has been successfully infiltrated. In doing this, they found that the presence of a surveillance message in the compromised computer systems decreased the probability of commands being typed in the system during longer first system trespassing incidents (Wilson, Maimon, Sobesto, & Cukier, 2015). Further, they found that the probability of commands being logged during subsequent system trespassing incidents (on the same target computer) is influenced by the presence of a warning banner and by whether commands have been entered during previous attacks (Wilson, Maimon, Sobesto, & Cukier, 2015). An attack is the logging of one or more keystroke commands.

Prior to Maimon and colleagues' (2014) study there were no empirical works examining restrictive deterrence in cyberspace; however, a growing body of literature in the realm of cyberdefense has investigated the utility of deterrent strategies involving denial of attack (Goodman, 2010). Cyberdefense deterrent strategies seek to deter through target hardening.

In addition, Goodman (2010) used real-world cases to demonstrate that it is possible to deter cyber attacks as long as the intent to enforce penalties is known by the potential offender. However, there are numerous problems concerning deterrence in cyberspace. Furnell (2002) found that law regarding cybercrime was unknown to the hacking community. This is problematic because people cannot be deterred by the threat of sanction if they do not know their actions are punishable (Beccaria, 1963 [1764]). Moreover, even those who recognize the illegality of system trespassing are not likely to be deterred due to the lack of stigma attached to computer crimes (Taylor, 1999; Yar, 2005). In fact, Yar (2005) states that a significant amount of youth participate in computer crime, and many deem it socially acceptable. Similarly, Taylor (1999) states that many believe hacking is a mere phase, in which active youth will mature out. Although previous studies found that stigma does not deter cybercrime as it does some crimes in the physical world (Yar, 2005), the work of Goodman (2010), Maimon and colleagues (2014), Jones (2014), and Wilson and colleagues (2015) contend that these crimes can be deterred in other ways.

Deterrence in cyberspace is also undermined by hackers' lack of fear for legal sanctions. It is well known within the hacking community that the criminal justice system lacks the ability to effectively police cybercrime (Choi, 2010). More specifically, Choi (2010) provided an empirical examination of routine activity theory in cyberspace and found that cyberspace lacks a capable guardian. By introducing warning banners that are suggestive of a capable guardian, the current study is able to offer a unique analysis of restrictive deterrence on post-compromised systems that extends beyond the scope of the Choi (2010) study.

Conversely, there is evidence in the literature that shows hackers utilize particularistic restrictive deterrence tactics similar to those described by Jacobs (1996a). More specifically, it is not uncommon for hackers to hide their identity through looping, using one computer to access another, and then another, and so on (Jones, 2014). Similarly, hackers often erase traces of their trespassing and create a backdoor into the system, thus allowing them to freely re-enter without being noticed (Wang, 2006). Wang (2006) found that oftentimes hackers do this by gaining control of the system administrator's account. Once hackers have gained control of the system administrator's account they can more easily make desired modifications.

These findings, along with the findings of Maimon and colleagues (2014) and Jones (2014) suggest the need for greater investigation into the restrictive deterrence techniques used by system trespassers. Criminologists have virtually ignored particularistic restrictive deterrence in cyberspace. The current study seeks to partially fill this gap in the literature by examining the temporal order of specific keystroke commands (a special set of keys that execute a command) that are logged by system trespassers during an intrusion. Examining the temporal order of these keystroke commands in relation to the treatment or control conditions allows us to examine the extent to which system trespassers modify their behavior after encountering various warning messages. This is a unique test of particularistic restrictive deterrence.

The Current Study

As discussed above, Jones (2014) expanded upon the Maimon and colleagues (2014) study in various ways. Most influential for the progression of the current study was her ability to examine the frequency of individual keystroke commands. In addition, she divided the commands into three categories based on their general functions: change commands, reconnaissance commands, and fetch commands (Jones, 2014). Change commands "change files, access permissions, or process on the computer" (Jones, 2014, p. 26). The commands included are adduser/useradd, passwd, chmod, rm –rf, touch, and kill/killall. Fetch commands are designed to do as the name suggests and "fetch files from other networks and bring them to the compromised computer" (Jones, 2014, p. 26). The commands included are wget, tar, and ftp. Reconnaissance commands, as defined by Jones (2014), are used to "report information about the computer's contents and processes" (p. 26). The commands included are w, uname, ps, uptime, and Is. Table 1 displays all of the aforementioned commands and their purpose.

Table 1. Command List

Command	**Command Description**
adduser/useradd	Creates a new user account
Passwd	Changes the password
Chmod	Changes access permissions
rm –rf	Removes files and/or directories.
Touch	Creates new, empty files and is used to change timestamps
kill/killall	Terminates processes
Wget	Downloads files
Tar	Extracts files
ftp	Transfers files from or to a remote network
W	Shows whether other users are logged into the system and their activity
Uname	Reports basic information about the computer's hardware and software
Ps	Reports on current processes
Uptime	Shows whether other users are logged on and how long the system has been running
Is	Lists all files

As seen in Table 1, the information reported by the various reconnaissance commands can be associated with the perceived probability of detection. In other words, a hacker may use reconnaissance commands to scope out the existence of a capable guardian in the same fashion a burglar checks to see if someone is home before breaking and entering. Similar to the burglar, the system trespasser is likely to become more cautious as his fear of detection increases; therefore, reconnaissance commands are employed by system trespassers as a tactical skill to avoid detection.

The grouping of these various commands has additional importance that expands beyond the scope of the Jones (2014) study. More specifically, it allows for the examination of particularistic restrictive deterrence in cyberspace after exposure to three individual warning banners: an altruistic message used for moral persuasion (warning 1), a legal sanction threat (warning 2), and an ambiguous threat (warning 3). As defined above, particularistic restrictive deterrence is the modification of behavior based on "tactical skills offenders use that make them less likely to be apprehended" (Jacobs, 1996a, p. 425).

Although not specifically tested, partial support for the existence of particularistic restrictive deterrence in cyberspace was found in Cherbonneau and Copes' (2006) study, which determined that system trespassers modify their behavior by logging specific commands to conceal their activity. In addition, Kigerl (2014) found that spammers take extra precautions when they feel that their identity is at risk of exposure. Moreover, Jones (2014) found that hackers who encounter the altruistic message are less likely than those who encounter the legal sanction threat or ambiguous threat to log any of the aforementioned reconnaissance commands; however, this finding was not pronounced enough to obtain statistical significance. A more effective measure of particularistic restrictive deterrence, which is tested within the current study, is the temporal order in which reconnaissance commands are logged. As we know from the literature on deterrence in the physical world, the effects of deterrence fades as offenders' perceived certainty of punishment decreases (Pogarsky, Piquero, & Paternoster, 2004). Therefore, it is intuitive that hackers will employ tactical skills in the early stages of their attack. More specifically, hackers who are more concerned with detection will log reconnaissance commands sooner than those less concerned with detection.

Due to the nature of the study I can only speculate on the reasons some hackers are more concerned with detection than others. However, I can use theory and prior research to guide my speculations. For example, Beccaria (1963 [1764]) contended that people cannot be deterred by the threat of sanction if they do not know their actions are punishable. Therefore, it is likely that those who are presented with a legal sanction threat will be more concerned with detection than those in the control group due to their increased awareness of the illegality of system trespassing and their perceived notion of a capable guardian. Moreover, prior research suggests that ambiguity increases the perceived certainty of sanctions (Kahneman and Tversky, 1979; Loughran et al., 2011); therefore, hackers who receive the ambiguous threat should also be more concerned with detection than those in the control group.

The Jones (2014) study demonstrates that the altruistic message has a probabilistic rather than a particularistic restrictive deterrent effect. Moreover, system trespassers who encounter the altruistic message are not given an adequate reason to fear detection. Attempting to use moral persuasion to deter system trespassing may even serve as an indicator that the system lacks a capable guardian. Therefore, I am inclined to speculate that hackers who encounter the altruistic message will be less concerned with detection than those in the control group. In other words, system trespassers in the control group will utilize reconnaissance commands at an earlier stage in their attack than those who encounter the altruistic message aimed at moral persuasion.

These speculations, which are grounded in theory and prior research, lead to the following hypotheses:

1. System trespassers who encounter the legal sanction threat will log a reconnaissance command at an earlier stage in their attack than system trespassers in the control group.
2. System trespassers who encounter the ambiguous threat will log a reconnaissance command at an earlier stage in their attack than system trespassers in the control group.
3. System trespassers who encounter the legal sanction threat will log a reconnaissance command at an earlier stage in their attack than system trespassers who encounter the altruistic message.
4. System trespassers who encounter the ambiguous threat will log a reconnaissance command at an earlier stage in their attack than system trespassers who encounter the altruistic message.
5. System trespassers who do not encounter a warning banner (the control group) will log a reconnaissance command at an earlier stage in their attack than system trespassers who encounter the altruistic message.

Methodology

Procedure

Maimon and colleagues (2014) conducted a pilot experiment, which examined attackers' post-compromised behavior using one experimental condition (the presence of a standard legal warning) and one control condition (no warning message). The warning banner used in the original study addressed the legality of system trespassing. Due to the success of the study, two additional treatment groups were included and tested on both American and non-American network infrastructures using honeypot computers.

A honeypot computer, as defined by Spitzner (2003) is, "a security resource whose value lies in being probed, attacked, or compromised" (p. 3). Honeypot computers are designed to be easy prey for system trespassers, with slight modification that allows activity to be logged (Even, 2000). It is believed that once a system is compromised, intruders will make subsequent visits, thus making honeypot computers ideal for collecting data (Even, 2000).

The current study utilizes the same dataset used in the Jones (2014) study, which was gathered from a Chinese University computer network, where 295 high-interaction honeypots were set up. Similar to the Maimon and colleagues (2014) study, the target computers were programed to exhibit or not to exhibit a warning banner once hackers had successfully infiltrated the systems. Building on Maimon and colleagues (2014) study, the current study utilizes three warning banners: an altruistic message used for moral persuasion (warning 1), a legal sanction threat (warning 2), and an ambiguous threat (warning 3) (see Appendix for banner content).

To ensure endogeneity, system trespassers were randomly assigned to the four conditions once they attempted to gain access by means of brute force (guessing the password a predetermined number of times). For the current study, the threshold was set to be a random number between 150 and 200 to emulate an authentic attack. Once access was granted to the honeypot systems, all of which ran Linux Ubuntu 9.10 with a modified version of an OpenSSH server. Intruders were allowed access to the honeypot computer for a period of thirty days, and were free to use the computer as they pleased. However, a firewall was employed to prevent hackers from engaging in activities harmful to other devices. Keystrokes were logged using the Sebek keylogger. After the thirty-day access period trespassers were kicked off the honeypot computer, it was cleaned, and redeployed.

Data

The honeypot computers were compromised 1,548 times, 478 of which the hackers executed an attack (logged 1 or more keystroke command). Since the modification of behavior can only be examined where behavior exists, the 478 attacks became the total sample. Of the total sample, 132 were not exposed to a warning banner (control group), 81 were exposed to the altruistic message, 135 to the legal warning, and 130 to the ambiguous threat. Table 2 displays the frequency of overall command usage. As seen in table 2, the median number of commands logged is five, the mean number is 7.55, and the first quartile falls at two commands logged. Therefore, the current study conceptualizes the early use of a reconnaissance command as the first or second command logged.

Table 2. Descriptive Statistics: Frequency of Command Usage

Mean	7.55
Median	5
Range	43
First Quartile	2

Analytic Strategy

To test the various hypotheses two dummy variables were created for each of the five reconnaissance commands. The first dummy variable indicates that the specific reconnaissance command was the first command logged by the system trespasser. The second dummy variable indicates that the specific reconnaissance command was the first or second command logged by the system trespasser. The dummy variables were then used to create a measure for all reconnaissance commands logged first, and another measure for all reconnaissance commands logged first or second. In other words, the current study first examined the reconnaissance commands individually then examined their combined significance.

Using the chi-square test of significance the current study was able to determine whether a significant difference exists between the expected frequencies and the observed frequencies in the various treatment groups. Similarly, by running a series of logistic regressions the present study was able to measure the relationship between logging a reconnaissance command at an early stage within an attack (the dependent variable) and the different warning banners (the independent variable). More specifically, the current study was able to determine which, if any, of the warning banners were associated with a higher rate of reconnaissance commands logged early in the attack.

In total, 12 measures of the dependent variable are included within the analyses (two for each of the five reconnaissance commands and the two summated measures). Since the data were collected using a randomized experimental design control variables are not included, nor are they needed.

Results

Table 3 presents the results (as percentages) of a series of bivariate cross-tabulations between honeypot type and the early use of various reconnaissance commands. The Chi-square test of significance did not yield statistically significant results; however, noteworthy findings exist throughout the analysis. Regarding the first two hypotheses, hackers who encounter the legal or ambiguous message are more likely to log a reconnaissance command at an early stage in their attack than those in the control group for seven of the twelve variables examined. Similarly, hackers who receive the legal sanction threat are more likely to log a reconnaissance command at an early stage in their attack than those who receive the altruistic message for seven of the twelve variables examined. Addressing the fourth hypothesis, hackers who receive the ambiguous threat are more likely to log a reconnaissance command at an early stage in their attack than those who receive the altruistic message for eight of the twelve variables examined. Lastly, addressing the fifth hypothesis, hackers in the control group are more likely to log a reconnaissance command at an early stage in their attack than those who encounter the altruistic message for eight of the twelve variables examined. Although none of which are statistically significant, the majority of findings are in the anticipated direction. In other words, the current study’s hypotheses accurately predicted which warning banners most influence the early use of reconnaissance commands.

A more in depth consideration of the percentages provide additional interesting findings. For example, 70% of those who receive the standard legal warning log a reconnaissance command as the first or second command within their attack, which is the large majority. An examination of individual commands show that some commands are used a great deal more than others across all of the treatment groups. For example, 46% of those who receive the ambiguous threat log W as the first or second command within their attack, whereas only 5% log Uptime. This is interesting because, as seen in Table 1, both commands inform the hacker on whether or not anyone else is logged onto the system. The decreased usage of the other reconnaissance commands is more intuitive since they do not directly relate to the existence of a capable guardian.

Table 4 displays the results of a series of logistic regressions. Support for the hypotheses were not found. As seen below, the various logistic regression models lack statistical significance, with the only significant finding being that those who encounter the ambiguous threat are more likely to log uname as the first command within their attack (b=2.15, SE=1.07, *p*=0.044). In other words, encountering the ambiguous threat in comparison to not encountering a warning banner increases the odds of logging uname as the first command within an attack by 758.49%. However, it is likely that this finding gained statistical significance due to the small percentage of hackers who logged the command. It was only logged 17 times, which is the least of any of the various reconnaissance commands.

Table 3. Percent of Command Usage: Bivariate Cross-Tabulations

Command Name	**Control**	**Altruistic**	**Legal**	**Ambiguous**
Recon 1st	61%	56%	62%	62%
Recon 1st or 2nd	66%	67%	70%	68%
W 1st	40%	37%	38%	42%
W 1st or 2nd	44%	41%	42%	46%
Uname 1st	1%	5%	3%	6%
Uname 1st or 2nd	11%	9%	13%	12%
Ps 1st	11%	9%	7%	5%
Ps 1st or 2nd	20%	19%	14%	12%
Uptime 1st	3%	4%	3%	4%
Uptime 1st or 2nd	3%	6%	4%	5%
Is 1st	7%	5%	11%	7%
Is 1st or 2nd	18%	15%	26%	18%

Table 4. Logistic Regression Output

<table>
<tr><th>Command name</th><th>Altruistic</th><th>Legal</th><th>Ambiguous</th></tr>
<tr><td>Recon 1st</td><td>Coef: -.189
Std. Err.: .287
P>|z|: 0.509</td><td>Coef: .036
Std. Err.: .252
P>|z|: 0.885</td><td>Coef:.007
Std. Err.: .254
P>|z|: 0.977</td></tr>
<tr><td>Recon 1st or 2nd</td><td>Coef: .034
Std. Err.: .299
P>|z|: 0.910</td><td>Coef: .206
Std. Err.: .263
P>|z|: 0.434</td><td>Coef: .116
Std. Err.: .263
P>|z|: 0.660</td></tr>
<tr><td>W 1st</td><td>Coef: -.131
Std. Err.: .291
P>|z|: 0.651</td><td>Coef: -.100
Std. Err.: .251
P>|z|: 0.691</td><td>Coef: .057
Std. Err.: .252
P>|z|: 0.819</td></tr>
<tr><td>W 1st or 2nd</td><td>Coef: -.131
Std. Err.: .286
P>|z|: 0.647</td><td>Coef: -.070
Std. Err.: .247
P>|z|: 0.777</td><td>Coef: .089
Std. Err.: .248
P>|z|: 0.719</td></tr>
<tr><td>Uname 1st</td><td>Coef: 1.92
Std. Err.: 1.13
P>|z|: 0.089</td><td>Coef: 1.39
Std. Err.: 1.12
P>|z|: 0.218</td><td>Coef: 2.15
Std. Err.: 1.07
P>|z|: 0.044*</td></tr>
<tr><td>Uname 1st or 2nd</td><td>Coef: -.227
Std. Err.: .486
P>|z|: 0.64</td><td>Coef: .194
Std. Err.: .384
P>|z|: 0.613</td><td>Coef: .095
Std. Err.: .394
P>|z|: 0.810</td></tr>
<tr><td>Ps 1st</td><td>Coef: -.227
Std. Err.: .486
P>|z|: 0.641</td><td>Coef: -.394
Std. Err.: .433
P>|z|: 0.363</td><td>Coef: .735
Std. Err.: .481
P>|z|: 0.126</td></tr>
<tr><td>Ps 1st or 2nd</td><td>Coef: -.076
Std. Err.: .360
P>|z|: 0.832</td><td>Coef: -.404
Std. Err.: .330
P>|z|: 0.222</td><td>Coef: -.558
Std. Err.: .345
P>|z|: 0.106</td></tr>
<tr><td>Uptime 1st</td><td>Coef: .208
Std. Err.: .777
P>|z|: 0.789</td><td>Coef: -.023
Std. Err.: .718
P>|z|: 0.974</td><td>Coef: .247
Std. Err.: .683
P>|z|:0.718</td></tr>
<tr><td>Uptime 1st or 2nd</td><td>Coef: .744
Std. Err.: .686
P>|z|: 0.278</td><td>Coef: .398
Std. Err.: .657
P>|z|: 0.545</td><td>Coef: .599
Std. Err.: .639
P>|z|: 0.348</td></tr>
<tr><td>Is 1st</td><td>Coef: -.343
Std. Err.: .618
P>|z|: 0.580</td><td>Coef: .536
Std. Err.: .441
P>|z|: 0.224</td><td>Coef: .016
Std. Err.: .488
P>|z|: 0.973</td></tr>
<tr><td>Is 1st or 2nd</td><td>Coef: -.245
Std. Err.: .386
P>|z|: -0.64</td><td>Coef: .454
Std. Err.: .299
P>|z|: 0.129</td><td>Coef: .019
Std. Err.: .319
P>|z|: 0.953</td></tr>
</table>

* *P* < 0.05

Discussion

System trespassing, the unauthorized access of computer systems, has become a worldwide phenomenon, which costs the global economy $400 billion annually (McAfee, 2014). Despite the growing concern criminologists remained relatively silent until Maimon and colleagues' (2014) study. Maimon and colleagues (2014) sparked criminological interest by finding that a warning banner significantly increases the rate of first system trespassing termination, and decreases the duration of first trespassing incidents. These findings were interpreted as preliminary evidence for the relevance of restrictive deterrence in cyberspace.

Jones (2014) expanded upon Maimon and colleagues' (2014) study by examining the influence of three warning banners on system trespassers' behavior: an altruistic message used for moral persuasion (warning 1), a legal sanction threat (warning 2), and an ambiguous threat (warning 3). More specifically, she examined the effects of the different warning banners on individual keystrokes. Interestingly, she found that the altruistic message has a deterrent effect, whereas the legal sanction threat and ambiguous threat do not. However, most influential to the current study was her grouping of the various keystroke commands.

Jones (2014) divided the commands into three categories based on their general functions: change commands, reconnaissance commands, and fetch commands. Due to their theoretical relevance the current study only focuses on reconnaissance commands, which are used to "report information about the computer's contents and processes" (Jones, 2014, p. 26). Given their intended purpose, reconnaissance commands can be associated with perceived probability of detection. In other words, a hacker may use reconnaissance commands to check for a capable guardian in cyberspace the same way a burglar checks for a capable guardian in the physical world. Similar to the burglar, system trespassers are likely to become more cautious as their fear of detection increases; therefore, reconnaissance commands are employed by system trespassers as a tactical skill to avoid detection. The most effective measure of particularistic restrictive deterrence, which is tested within the current study, is the temporal order in which reconnaissance commands are logged. It is intuitive that hackers who are more concerned with detection will log reconnaissance commands sooner than those less concerned with detection. Drawing from theory and prior research (as discussed above), the following hypotheses were developed:

1. System trespassers who encounter the legal sanction threat will log a reconnaissance command at an earlier stage in their attack than system trespassers in the control group.
2. System trespassers who encounter the ambiguous threat will log a reconnaissance command at an earlier stage in their attack than system trespassers in the control group.
3. System trespassers who encounter the legal sanction threat will log a reconnaissance command at an earlier stage in their attack than system trespassers who encounter the altruistic message.
4. System trespassers who encounter the ambiguous threat will log a reconnaissance command at an earlier stage in their attack than system trespassers who encounter the altruistic message.
5. System trespassers who do not encounter a warning banner (the control group) will log a reconnaissance command at an earlier stage in their attack than system trespassers who encounter the altruistic message.

The current study utilizes the same dataset used in the Jones (2014) study, which was gathered from a Chinese University computer network, where 295 high-interaction honeypots were set up. The honeypot computers (computers designed to be attacked in order to collect data) were programed to randomly exhibit or not to exhibit a warning banner once hackers had successfully infiltrated the systems. The current study utilizes three warning banners: an altruistic message used for moral persuasion (warning 1), a legal sanction threat (warning 2), and an ambiguous threat (warning 3).

In total the honeypots were compromised 1,548 times, 478 of which the hackers executed an attack (logged 1 or more keystroke command). The 478 attacks became my total sample since the modification of behavior can only be examined where behavior exists. Of the total sample, 132 were not exposed to a warning banner (control group), 81 were exposed to the altruistic message, 135 to the legal warning, and 130 to the ambiguous threat.

To test the aforementioned hypotheses two dummy variables were created for each of the five reconnaissance commands. The first dummy variable indicates that the reconnaissance command was the first command logged, and the second dummy variable indicates that the reconnaissance command was the first or second command logged. Two additional dummy variables were created. The first indicates that any of the reconnaissance commands were the first command logged, and the second indicates that any of the reconnaissance commands were the first of second command logged. In total, the analyses have 12 dependent variables (two for each of the five reconnaissance commands, and two summated measures).

A series of bivariate cross tabulations were run to determine whether a significant difference exists between the expected frequencies and the observed frequencies in the various treatment groups. Similarly, a series of logistic regressions were run to measure the relationship between logging a reconnaissance command at an early stage within an attack (the dependent variable) and the different warning banners (the independent variable).

Although the bivariate cross tabulations did not yield statistically significant results, the majority of findings are in the anticipated direction. In other words, the current study's hypotheses accurately predicted which warning banners most influence the early use of reconnaissance commands. The various logistic regression models also lacked statistical significance, with the only significant finding being that those who encounter the ambiguous threat are more likely to log uname as the first command within their attack, which is likely due to the limited number of hackers who logged this specific command. Therefore, the logistic regression models do not provide support for the hypotheses.

Although the current study lacks statistical significance, it adds to that found by Maimon and colleagues (2014) and Jones (2014) by examining tactical skills that hackers use to avoid detection. Research aimed to examine hackers' behavior can inform those working in cyber security whilst adding to a relatively new body of literature; however, additional studies are imperative.

A post hoc speculation is that the current study may have failed to obtain statistical significance due to various limitations within the study, in which future research should attempt to address. As previously mentioned, the current study's data were collected from a Chinese computer system, which may prevent a percentage of hackers from being able to read the content of the warning banners. If the hackers were not able to understand the message, it is intuitive that it would not have deterred them.

In addition, the unit of analysis in the current study is the attack rather than the hacker, which limits the study in various ways. For example, it is possible that the same hacker compromised more than one honeypot, which threatens the validity of the study due to the possibility that a hacker encountered more than one warning banner. Additional analyses aimed to examine the diminishing effects of warning banners on hackers' behavior during subsequent attacks would have made for a stronger study; however, this was not possible given that different hackers could potentially hack from the same IP address, and that the same hacker could potentially hack from different IP addresses. Future studies should examine the initial attack separately, as it is more likely that the deterrent effect will be pronounced.

It is also likely that the current study failed to yield statistical significant results due to the deterrent effect that was observed in Maimon and colleagues' (2014) study and Jones' (2014) study. More specifically, it is likely that those who would have utilized tactical skills to avoid detection were instead completely deterred from logging any keystroke command. Therefore, it is possible that the current study failed to capture existing restrictive deterrent effects due to a biased sample. Although it is not possible to conclude with any certainty, a plausible speculation is that inherent differences exist between those who encountered a warning banner and decided to attack the compromised computer and those who did not. Future studies should attempt to parse out these differences.

Lastly, future studies should examine other tactical skills that hackers use to avoid detection. It is entirely possible that hackers avoid detection in a number of ways. Better understanding the ways in which hackers avoid detection will not only advance scientific knowledge, but also inform system administrators on ways to protect their system from becoming compromised.

References

Appel, J. B., & Peterson, N. J. (1965). What's wrong with punishment? *Journal of Criminal Law and Criminology*, *56*(4), 450-453.

Beccaria, C. (1963). *On crimes and punishments* (introduction by H. Paolucci, Trans.). New York: Macmillan. (Original work published 1764)

Becker, C. (1968). Crime and punishment: An economic approach. *Journal of Political Economy, 76*(2), 169-217.

Bentham, J. (1948). *An introduction to the principles of morals and legislation*. New York, NY: Hafner Publishing Company. (Original work published 1789)

Burt, Cyril. (1925). *The young delinquent.* London: University of London Press.

Cherbonneau, M., & Copes, H. (2006). 'Drive it like you stole it': Auto theft and the illusion of normalcy. *British Journal of Criminology*, *46*(2), 193-211.

Choi, K. S. (2010). *Risk factors in computer-crime victimization*. El Paso, TX: LFB Scholarly Publishing.

Clarke, R. V. G. (Ed.). (1997). *Situational crime prevention*. Monsey, NY: Criminal Justice Press.

Clarke, R. V. G., & Cornish, D. B. (Eds.). (1983). *Crime control in Britain: A review of policy research*. Albany, NY: SUNY Press.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*(4), 588-608.

Coleman, S. (2007). *The Minnesota income tax compliance experiment: Replication of the social norms experiment.* MPRA Paper 5820. Munich, Germany: Munich University Library.

Cromwell, P. F., & Olson, J. N. (2004). *Breaking and entering: Burglars on burglary*. Belmont, CA: Thomson/Wadsworth.

Decker, J. F. (1972). Curbside deterrence?: An analysis of the effect of a slug-rejector device, coin-view window, and warning labels on slug usage in New York City parking meters. *Criminology*, *1*(2), 127-142.

Eck, J. E., & Wartell, J. (1998). Improving the management of rental properties with drug problems: A randomized experiment. *Crime Prevention Studies*, *9*, 161-185.

Even, L.R. (2000) *Honey pot systems explained*. Retrieved from http://www.sans.org/resources/idfaq/ honeypot3.php.

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. London: Addison-Wesley.

Gabor, T. (1990). Crime displacement and situational prevention: Toward the development of some principles. *Canadian Journal of Criminology*, *32*(1), 41-73.

Gallupe, O., Bouchard, M., & Caulkins, J. P. (2011). No change is a good change?: Restrictive deterrence in illegal drug markets. *Journal of Criminal Justice*, *39*(1), 81-89.

Geerken, M. R., & Gove, W. R. (1975). Deterrence: Some theoretical considerations. *Law & Society Review*, *9*(3), 497-513.

Gibbs, J. P. (1968). Crime, punishment, and deterrence. *The Southwestern Social Science Quarterly*, *48*(4), 515-530.

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

Goffman, E. (1963). *Behavior in public places: Notes on the social organization of gatherings*. New York, NY: Free Press.

Goodman, W. (2010). Cyber deterrence: Tougher in theory than in practice? *Strategic Studies Quarterly, 4*(3), 102-135.

Grabosky, P. N. (1996). Unintended consequences of crime prevention. *Crime Prevention Studies*, *5(1)* , 25-56.

Grandjean, C. (1990). Bank robberies and physical security in Switzerland: A case study of the escalation and displacement phenomena. *Security Journal*, *1*(3), 155-159.

Hartshorne, H., & May, M. A. (1928). *Studies in the nature of character. Vol. I: Studies in Deceit.* New York, NY: MacMillan.

Jacobs, Bruce A. (1993). Undercover deception clues: A case of restrictive deterrence. *Criminology 31*(2), 281-299.

Jacobs, Bruce A. (1996a). Crack dealers and restrictive deterrence: Identifying narcs. *Criminology 34*(3), 409-431.

Jacobs, Bruce A. (1996b). Crack dealers' apprehension avoidance techniques: A case of restrictive deterrence. *Justice Quarterly 13*(3), 359-381.

Jacobs, B. A., & Cherbonneau, M. (2014). Auto theft and restrictive deterrence. *Justice Quarterly*, *31*(2), 344-367.

Jacobs, Bruce A., and Miller, J. (1998). Crack dealing, gender and arrest avoidance. *Social Problems, 45*(4), 550–69.

Jeffery, C. Ray. (1971). *Crime prevention through environmental design*. Beverly Hills, CA: Sage.

Jones, H. M. (2014). The restrictive deterrent effect of warning messages on the behavior of computer system trespassers. (Doctoral dissertation).

Kigerl, A.C. (2014). Evaluation of the CAN SPAM ACT: Testing deterrence and other influences of e-mail spammer legal compliance over time. *Social Science Computer Review, 33*(4), 440-458.

Loughran, T. A., Paternoster, R., Piquero, A. R., & Pogarsky, G. (2011). On ambiguity in perceptions of risk: Implications for criminal decision making and deterrence. *Criminology*, *49*(4), 1029-1061.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica: Journal of the Econometric Society*, *47*(2), 263-291.

Lowman, J. (1992). Street prostitution control some Canadian reflections on the Finsbury Park experience. *British Journal of Criminology*, *32*(1), 1-17.

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.

Matza, D. (1964). *Delinquency and drift*. New York, NY: Wiley.

McAfee. (2014). Net losses: Estimating the global cost of cybercrime. Retrieved April 03, 2016, from http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

Mischel, W. (1968). *Personality and assessment*. New York, NY: Wiley.

Newman, O. (1972). *Defensible space: Crime prevention through urban design.* New York, NY: Macmillan. (Published in London: Architectural Press, 1973).

Paternoster, R. (1989). Absolute and restrictive deterrence in a panel of youth: Explaining the onset, persistence/desistance, and frequency of delinquent offending. *Social Problems*, *36*(3), 289-309.

Paternoster, R. (2010). How much do we really know about criminal deterrence? *The Journal of Criminal Law and Criminology*, *100*(3), 765-824.

Paternoster, R., & Simpson, S. (1996). Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law and Society Review*, *30*(3), 549-583.

Pogarsky, G., Piquero, A. R., & Paternoster, R. (2004). Modeling change in perceptions about sanction threats: The neglected linkage in deterrence theory. *Journal of Quantitative Criminology*, *20*(4), 343-369.

Ponemon Institute. (2013). *2013 Cost of cyber crime study: United States*. Retrieved April 03, 2016, from http://www.hpenterprisesecurity.com/ponemon-2013-cost-of-cyber-crime-study-reports.

Rämä, P., & Kulmala, R. (2000). Effects of variable message signs for slippery road conditions on driving speed and headways. *Transportation Research Part F: Traffic Psychology and Behaviour*, *3*(2), 85-94.

Rengert, G., & Wasilchick, J. (1989). Space, time, and crime: Ethnographic insights into residential burglary. *Final Report to the National Institute of Justice, US Department of Justice*.

Schwartz, R. D., & Orleans, S. (1967). On legal sanctions. *The University of Chicago Law Review*, *34*(2), 274-300.

Spitzner, L. (2003). *Honeypots: Definitions and value of honeypots*. Retrieved from http://www.tracking-hackers. com/papers/honeypots. html.

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,* 19-22.

Taylor, P. A. (1999). *Hackers*. London, UK: Routledge.

Tedeschi, J. T., & Felson, R. B. (1994). *Violence, aggression, and coercive actions.* Washington, DC: American Psychological Association.

Tizard, J., Sinclair, I., & Clarke, R. V. G. (Eds.). (1975). *Varieties of residential experience*. London: Routledge.

Toby, J. (1964). Is punishment Necessary? *The Journal of Criminal Law, Criminology, and Police Science*, *55*(3), 332-337.

Von Hentig, H. (1938). The limits of deterrence. *Journal of Criminal Law and Criminology (1931-1951)*, *29*(4), 555-561.

Wang, W. (2006). *Steal this computer book 4.0: What they won't tell you about the Internet*. No Starch Press.

Wilkins, L. T. (1964). *Social deviance: Social policy, action and research*. London: Tavistock Publications.

Wilkinson, P. (1986). *Terrorism and the liberal state.* Columbia, NY: New York University Press.

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*, *52*(6), 829-855.

Wright, R. T., & Decker, S. (1994). *Burglars on the job*. Boston, MA: Northeastern University Press.

Wright, R., & Decker, S. H. (1997). Creating the illusion of impending death: Armed robbers in action. *The Harry Frank Guggenheim Review*, *2*(1), 10-18.

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

Zimring, F. E., Hawkins, G., & Vorenberg, J. (1973). *Deterrence: The legal threat in crime control*. Chicago, IL: University of Chicago Press.

Appendix: Warning Banners

Altruistic Warning (Treatment 1):

Greetings friend,□We congratulate you on gaining access to our system, but must request that you not negatively impact our system.□Sincerely,□Over-worked admin

Standard Legal Warning (Treatment 2):

The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited. Unauthorized users are subject to Institutional disciplinary proceedings and/or criminal and civil penalties under state, federal, or other applicable domestic or foreign laws. The use of this system is monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and is advised that if monitoring reveals possible evidence of criminal activity, the Institution may provide evidence of such activity to law enforcement officials.

Ambiguous Warning (Treatment 3):

We have acquired your IP address.□Logout now and there will not be any consequences.