International Journal of Cyber Criminology
Vol 11 Issue 1 January – June 2017

System Trespasser Behavior after Exposure to Warning Messages at a Chinese Computer Network: An Examination

Christian J. Howell[1]
University of South Florida,
United States of America

David Maimon[2]
University of Maryland,
United States of America

John K. Cochran[3]
University of South Florida,
United States of America

Hattie M. Jones[4]
BBP Law School, United Kingdom

Ráchael A. Powers[5]
University of South Florida,
United States of America

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 three warning messages. 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.

Keywords: Anonymity, Cyber bullying, Demographics, Identity, Online Harassment, Perception, Psychological Stress, Social Networking Sites, Victimization.

[1] Graduate Student, Department of Criminology, University of South Florida, 4202 E. Fowler Ave., SOC 107, Tampa, FL 33620-8100, USA. Email: cjhowell@mail.usf.edu
[2] Associate Professor, Department of Criminology and Criminal Justice, University of Maryland, 2220 Samuel J. LeFrak Hall, 7251 Preinkert Drive, College Park, MD 20742, USA. Email: dmaimon@umd.edu
[3] Professor, Department of Criminology, University of South Florida, 4202 E. Fowler Ave., SOC 107, Tampa, FL 33620-8100, USA. Email: cochran@usf.edu
[4] BPP Law School, Whitehall, 2 Whitehall Quay, Leeds LS1 4HR, UK. Email: hattiejones89@gmail.com
[5] Assistant Professor, Department of Criminology, University of South Florida, 4202 E. Fowler Ave., SOC 107, Tampa, FL 33620-8100, USA. Email: powersr@usf.edu

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, 2015). Additionally, at the individual level, system trespassers (also known as hackers) can gain access to sensitive information, which can be used to facilitate 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.

Theoretical Background and Literature Review

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.

Deterrence theory was nearly discredited by the scientific community until two studies in 1968 revitalized criminological interest in the theory (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 occurs after weighing the costs and benefits of committing a crime against the costs and benefits of 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. 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.

In other instances, referred to as restrictive deterrence, the threat of legal sanctions does not cause individuals to abstain fully from crime, but instead causes individuals to curtail or modify their criminal behavior to reduce the risk of punishment (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).

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.

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 choose 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 of the criminal act (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.

In addition, 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.

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; Rämä & Kulmala, 2000). For example, warning banners have no effect on prostitution (Loman, 1992), yet decrease unsafe driving (Rämä & 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 of deterrence through warning banners to cyberspace.

Deterrence in Cyberspace

Although an immense body of restrictive deterrence literature has accumulated, criminologists had 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 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 and 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 et al., 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) found that the presence of a surveillance message in compromised computer systems decreased the probability of commands being typed in the system during longer first system trespassing incidents (Wilson et al., 2015). Further, they found that the presence of a warning banner decreased the probability of commands being logged during subsequent system trespassing incidents (Wilson et al., 2015). 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 cyber defense has investigated the utility of deterrent strategies involving denial of attack (Goodman, 2010). Cyber defense 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 cyber crime laws were unknown to the hacking community. This is problematic because potential offenders 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 cyber crime 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) contends 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 cyber crime (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) study and Jones (2014) study, 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.

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).

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

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 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, we can only speculate the reasons some hackers are more concerned with detection than others. However, we can use theory and prior research to guide these 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 & Tversky, 1979; Loughran, Paternoster, Piquero, &

Pogarsky, 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, we are inclined to postulate 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

Maimon and colleagues (2014) conducted a pilot experiment that 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 is, as defined by Spitzner (2003), "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, in which 295 high-interaction honeypots were set up. Similar to the Maimon and colleagues (2014) study, the target computers were programed to exhibit or not 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, which was subsequently 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 indicated that the specific reconnaissance command was the first command logged by the system trespasser. The second dummy variable indicated 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 neither necessary nor included.

Results

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 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.

Table 4: Logistic Regression Output

Command Name	Altruistic			Legal			Ambiguous		
	B	*SE*	$p>\|z\|$	*B*	*SE*	$p>\|z\|$	*B*	*SE*	$p>\|z\|$
Recon 1st	-0.189	0.287	0.509	0.036	0.252	0.885	0.007	0.254	0.0977
Recon 1st or 2nd	0.034	0.299	0.910	0.206	0.263	0.434	0.116	0.263	0.66
W 1st	-0.131	0.291	0.651	-0.100	0.251	0.691	0.057	0.252	0.819
W 1st or 2nd	-0.131	0.286	0.647	-0.070	0.247	0.777	0.089	0.248	0.719
Uname 1st	1.920	1.130	0.089	1.390	1.120	0.218	2.150	1.070	0.044★
Uname 1st or 2nd	-0.227	0.486	0.640	0.194	0.384	0.613	0.095	0.394	0.810
Ps 1st	-0.227	0.486	0.641	-0.394	0.433	0.363	0.735	0.481	0.126
Ps 1st or 2nd	-0.076	0.360	0.832	-0.404	0.330	0.222	−0.558	0.345	0.106
Uptime 1st	0.208	0.777	0.789	-0.023	0.718	0.974	0.247	0.683	0.718
Uptime 1st or 2nd	0.744	0.686	0.278	0.398	0.657	0.545	0.599	0.639	0.348
Is 1st	-0.343	0.618	0.580	0.536	0.441	0.224	0.016	0.488	0.973
Is 1st or 2nd	-0.245	0.386	-0.640	0.454	0.299	0.129	0.019	0.319	0.953

★ $p < 0.05$

A more in depth consideration of the percentages provides 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.

Discussion and Conclusion

The current study examined the temporal order of various keystroke commands to determine if some keystroke commands are used as a tactical skill to avoid detection. The lack of statistical significance within the study does not serve as proof that particularistic restrictive deterrence does not exist in cyber space. Instead, a thoughtful post hoc analysis exemplifies certain limitations within the study, which may have masked its relevance. For example, the current study's data were collected from a Chinese computer system, which may have prevented 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 to infer that it did not deter 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. Moreover, Chan and Yao (2005) found that hackers are deterred by varying degrees based on their motivation to hack. More specifically, a hacker is less likely to be deterred when intrinsically motivated (Chan & Yao, 2005). The current study was unable to examine the hackers' motivation.

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 statistically 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. In addition, those who were not initially deterred likely placed greater emphasis on the perceived benefits than the perceived risks. 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

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.

Chan, S. H., & Yao, L. J. (2005). An empirical investigation of hacking behavior. *Review of Business Information Systems*, *9*(4), 41-58.

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.

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). *Cyber crime: Vandalizing the information society*. London: Addison-Wesley.

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.

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

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

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

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

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

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.

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.

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

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.

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. (2015). *2015 Cost of cyber crime study: United States.* Retrieved April 03, 2016, http://www.ponemon.org/blog/2015-cost-of-cyber-crime-united-states.

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*.

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.

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

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.