ABSTRACT

Title of thesis: THE RESTRICTIVE DETERRENT EFFECT OF WARNING MESSAGES ON THE BEHAVIOR OF COMPUTER SYSTEM TRESPASSERS

Harriet Mary Jones. Master of Arts. 2014

Thesis directed by: Dr David Maimon

Department of Criminology and Criminal Justice

Computer system trespassing is a growing concern, but it has received little criminological attention. The present study discusses the results of an experiment which looked at system trespasser behavior after exposure to one of three warning messages (or no message) in the context of deterrence theory. One message consisted of an attempt at moral persuasion; the second a generic legal warning, and the third an ambiguous threat. Keystroke data was analyzed to assess how the type of message affected the employment of restrictive deterrent techniques designed to limit trespasser activity on a compromised system. It was found that moral persuasion generally reduces both the incidence and frequency of command entry by trespassers on an illegally accessed system, while legal and ambiguous warnings produce no significant differences from the control condition. This suggests that in order to reduce trespasser activity, system administrators should use moral persuasion instead of legal sanction threats.

THE RESTRICTIVE DETERRENT EFFECT OF WARNING MESSAGES ON THE BEHAVIOR OF COMPUTER SYSTEM TRESPASSERS

by

Harriet Mary Jones

Thesis submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Master of Arts
2014

Advisory Committee:

Dr David Maimon, Chair

Professor Gary LaFree

Dr Thomas Loughran

TABLE OF CONTENTS

1. INTRODUCTION

Cybercrime is a growing problem worldwide with significant financial ramifications. Indeed the total cost to United States companies from cybercrime in 2013 has been estimated at $11,560,000, representing a 26% net increase in cost compared to the previous year (Ponemon Institute, 2013). Additionally, invasion of privacy has also become a common global problem, with almost one in five people in both the United States and the United Kingdom experiencing the hacking of an online account in the previous year (Bursztein, 2013; Hernandez-Castro and Boiten, 2013). However even these estimates of the extent of cybercrime probably understate the problem, since our knowledge of the true extent of cybercrime is impaired by the anonymous and boundless nature of cyberspace (Yar, 2006). Despite growing public awareness of the threat of privacy invasion and cyber attacks, there has been little concerted criminal justice effort to effectively counter cybercrime, and it has gone largely ignored within the field of criminology (Choi, 2011).

The few attempts to apply traditional criminological theory to cybercrime have for the most part explored computer victimization with reference to the Routine Activities Theory of Cohen and Felson (Choi, 2010, 2011; Cohen and Felson, 1979). By contrast, the current paper explores not criminal victimization but commission, investigating how deterrence theory might be applied to cyberspace. Specifically this work focuses on how sanction threats, in the form of warning banners, may affect the behavior of 'system trespassers' (those who illegally enter into a computer or network) after they have compromised and gained access to a computer system (their "post-compromise" behavior). Rather than using the classical model of deterrence, where the act either

proceeds in spite of or is omitted *in toto* because of a sanction threat, the focus in the present work is on exploring the more recent concept of restrictive deterrence (Gibbs, 1975; Jacobs, 1996a, 1996b, 2010) where the circumscribed behavior continues despite the sanction threat but responds to it in any one of a number of ways.

The present experiment consists of a randomized trial using a set of target-computers purpose-built for being attacked. Three experimental conditions were employed (one of three different warning banners displayed when a system trespasser enters the computer system for the first time) in addition to one control condition (no warning banner displayed). The three experimental conditions allow comparison of the ways in which an 'altruistic' appeal to morality, a threat of legal sanctions and an ambiguously threatening message affect trespasser behavior. This work is the first to look not only at the effects of warning banners on the progression of a system trespassing event but also at the individual-level keystroke data of system trespassers. It seeks to ascertain what type of warning message will result in a reduction of criminal activity on an illegally accessed computer system. It is hoped that the findings reached will inform policy on computer and network safety.

2. THEORETICAL BACKGROUND

2.1 System Trespassing

System trespassing involves the unauthorized entry into a computer or network by someone who does not have access rights (Brenner, 2010). Instead of 'system trespassing' the term 'hacking' (or 'cracking') is often used (Yar, 2006). System trespassers search for susceptible target computers through methods such as port

scanning, where they use the internet to look for open ports into networks which might provide points of entry into the system (Lee et al., 2003). Once the trespasser has gained unauthorized access to a system, either locally (by physically accessing it) or, more commonly, remotely (by utilizing an internet connection), the individual may conduct any number of a range of activities related to computer intrusion, manipulation and disruption (Yar, 2006).

The motivations attributed variously to system trespassers by law enforcement, the public and trespassers themselves have been described as "wide-ranging and often contradictory" (Yar, 2005:391). Law enforcement descriptions of the activities of system trespassers tend to focus on the malicious or destructive nature of certain acts, while trespassers themselves often characterize their actions as being conducted in the pursuit of knowledge and in support of freedom of information (Yar, 2005). All that can be stated with any certainty is that trespassers may enter systems for the purposes of exploration, information, sabotage or curiosity; to steal resources or information, store resources or information, alter or sabotage the system, deface websites, distribute malicious software, protest against restrictions on information, improve computer security by exposing flaws, flaunt their own skillset, gain recognition from other cybercriminals, make a political statement, feel powerful and in control, or any combination of these factors (Chiesa et al., 2009; Loader, 2000; Taylor, 1999; Yar, 2006).

Whatever motives are attributed to them, it seems that system trespassers are generally viewed by the law, the public and themselves as rational actors who engage in hacking with the expectation of some sort of reward (whether that be information, the

ability to perpetrate further attacks or to satiate curiosity) (Yar, 2005, 2006). This renders them theoretically open to being deterred by sanction threats. The legal response to system trespassing in the USA and other Western societies has been consistent with deterrence theory inasmuch as formal sanctions have been implemented in the hopes of deterring system trespassing - most notably through the American 1986 Computer Fraud and Abuse Act, which allows for up to ten years' imprisonment for computer offenses (Kerr, 2009).

2.2 Deterrence Theory

Deterrence theory has its roots in the writings of the 18th century philosophers Jeremy Bentham (1948 [1789]) and Cesare Beccaria (1963 [1764]) who proposed that humans were self-interested and rational-thinking, driven in their actions by an economical 'hedonistic calculus' whereby they act so as to maximize pleasure and minimize pain (Bentham, 1948 [1789]; Paternoster, 2010; Tombs and Whyte, 2013). This theoretically renders individuals open to 'deterrence' inasmuch as raising the costs of a behavior through sanctions should lower their willingness to pursue that course of action. Ultimately, the theory predicts that when the costs outweigh the benefits an individual should refrain from acting altogether (Beccaria, 1963 [1764]; Zimring and Hawkins, 1973).

Contemporary deterrence and rational choice scholarship has yielded six main areas of research development:

One is a more detailed consideration of Beccaria's (1963 [1764]) bifurcation of *specific* and *general* deterrence, where *specific* deterrence is the cessation or curtailment

of an individual's criminal activity in response to a legal sanction *applied* to the offender (Andenaes, 1974; Gibbs, 1975; Paternoster and Piquero, 1995), and *general* deterrence is the cessation or curtailment of criminal offending on the part of potential offenders due to the *prescription* of legal sanctions (combined with known enforcement of those sanctions) (Andenaes, 1966; Paternoster and Piquero, 1995). However work by Stafford and Warr (1993) suggests that the division is artificial and unnecessary, and that both direct (specific) and indirect (general) deterrence affect individual offenders (see for example Anwar and Loughran, 2011; Loughran et al., 2011a).

A second key development has been the recognition that most (if not all) individuals are incapable of employing the sort of pure mathematical cognitive process in decision-making implied by Beccaria (1963 [1764]) and that humans act with a rationality 'bounded' or limited by their lack of access to complete information (Cherniak, 1986; Simon, 1972). Indeed empirical research has shown that human decisions are affected by non-rational concerns such as the manner in which risks are described and miscalculations regarding cumulative probabilities of punishment (Casey and Scholtz, 1991; see also Loughran et al., 2011b).

A third development has been the adoption of a *perceptual* approach to the study of deterrence, where it has been recognized that measuring the individual's *perception* of the certainty and severity of punishment is more relevant to calculating a deterrent effect than merely measuring the objective risk or severity (Becker, 1968; Paternoster, 1987; Zimring and Hawkins, 1973). Pogarsky et al. (2004) indicated that objective sanctions are connected to behavioral outcomes through two separate links – a *perceptual* link between the sanction and the offender's perception about the risks and costs of punishment, and a

behavioral link between that perception and their behavior. Both of these must be present for an objective sanction to translate into deterrence. Empirical work has generally also found, consistent with Beccaria's (1963 [1764]) predictions, that perceived certainty of sanction has a greater deterrent effect than perceived severity of sanction (Anderson et al., 1977; Klepper and Nagin, 1989; Nagin and Pogarsky, 2001; Paternoster, 1987; Tittle, 1969; but see qualifications to this in Piquero and Pogarsky, 2002; Pogarsky, 2002).

Some recent work in the field of perceived certainty has examined the role of ambiguity in weakening or enhancing perceptions of certainty. Generally studies suggest that individuals are 'ambiguity adverse', preferring to gamble with known risks as opposed to uncertain ones (Loughran et al., 2011b). In line with evidence that human decision-making is not entirely rational (Simon, 1972), it has been found that ambiguity enhances the deterrent effect of low risks (Kahneman and Tversky, 1979; Shimizu, 2007). Casey and Scholz find evidence of a 'boundary effect', whereby vagueness makes tax noncompliance more attractive when the probability of detection is very high (>90%) but less attractive when the probability of detection is very low (<10%) (1991:838). In a more recent study, Loughran et al. (2011b) recalculate these boundary effects, also finding evidence that ambiguity enhances the deterrent effect of low risks (<20%), and reduces the deterrent effect of high risks (>80%).

Research on ambiguity of perceived severity is less developed, being largely intertwined with work on perceived certainty of loss or gain, but with general findings that it is the probability of gaining (as opposed to losing) rather than the size of the gain that has a greater influence on decision-making (Liu and Colman, 2009). However much of this work involves experimenting with differing levels of gain rather than with loss.

Recent work on loss aversion itself has found that people are risk-prone towards small potential losses or gains and risk-averse when confronted with large potential losses or gains (Bosch-Domènech and Silvestre, 2006). The premise of deterrence theory is that a legal sanction constitutes a relatively severe 'loss' and thus, when confronted with the potential for legal sanction, people will generally be risk-adverse. There is little research explicitly testing the effect of ambiguity of sanction level on human behavior in the absence of ambiguity of certainty, although Casey and Scholz's (1991) paper suggests that ambiguity of penalty severity has a similar effect to ambiguity of probability of detection. They found that ambiguity serves to increase the chances of noncompliance when the penalty estimate is high but reduces the chances of noncompliance when the penalty estimate is low. Thus ambiguity of perceived certainty and severity seem to operate in a largely similar and complementary manner.

A fourth area is that of the relative impact of *informal* sanctions as compared to the formal sanctions specified in the traditional deterrence model, with some work suggesting that the main deterrent effect of formal sanctions derives from the attendant informal sanctions suffered by individuals upon arrest or imprisonment such as social ostracization and shaming (Erickson et al., 1977; Kleck et al., 2005; Nagin and Pogarsky, 2001; Tittle and Rowe, 1974; Zimring and Hawkins, 1973).

Fifth, some work has examined *deterrability*, or how individual characteristics may render some people more or less susceptible to deterrence processes dependent upon their level of impulsivity, commitment to crime or future orientation (Chambliss, 1967; Nagin and Paternoster, 1993; Paternoster, 2010; Wright et al., 2004).

Finally, a sixth development has been the further bifurcation of deterrence into *absolute* and *restrictive* deterrence, proposed by Gibbs (1975) and further developed primarily by Jacobs (1993, 1996a, 1996b, 2010). Whilst the other developments in deterrence theory have some background importance to the way in which deterrent processes are conceptualized for the purposes of this study, the present work explicitly engages with and empirically assesses the relevance of restrictive deterrence in a cyber context.

2.3 Restrictive Deterrence

In his classic (1975) work, Gibbs differentiates between *absolute* and *restrictive* deterrence. *Absolute* deterrence essentially constitutes the classical model of deterrence, where an individual engages in no criminal activity due to the fear induced by some perceived risk of punishment. *Restrictive* deterrence, on the other hand, is the curtailment of a certain type of criminal activity at least in part in order to try and reduce the risk of punishment (Gibbs, 1975). Whilst Gibbs (1975) argued that restrictive deterrence is a function of specific deterrence, Jacobs (1996a) proposed that it might be a function of specific or general deterrence separately, or indeed both together. An individual does not, therefore, have to have suffered punishment themselves in order to experience restrictive deterrence.

The core idea of restrictive deterrence is that, if it is operative, one will see not the *omission* of an act but its *curtailment*. This was suggested by Gibbs (1975) to primarily constitute a reduction in the frequency of the act, with the expectation (based on a probabilistic style of decision-making) that less offending translates into fewer chances

for detection and arrest. However, later work by Jacobs (1993, 1996a) problematizes this assumption of 'probabilistic' restrictive deterrence. His ethnographic work with drug dealers suggests an absence of this "law of averages" mentality and reveals that criminals curtail their drug dealing primarily due to their employment of strategic tactics used to identify (and avoid) high-risk targets rather than any consideration of their long-term odds of punishment (Jacobs, 1993; see also Johnson and Natarajan, 1995; VanNostrand and Tewksbury, 1999). This builds on a footnote by Gibbs (1975) that suggests the potential for a reduction in offense frequency due to "any strategies or tactics employed by individuals to evade detection, identification, or apprehension" (Gibbs, 1975:33). Jacobs (1996a) labels this 'particularistic' restrictive deterrence.

Gibbs (1975) assumes that arrest avoidance strategies prompted by restrictive deterrence concerns will translate into less crime due to a reduction in frequency of offending. However Jacobs (1993) stresses that restrictive deterrence may not always effect a net reduction in crime, but in some instances may merely cause its displacement to other points in time and space that are perceived by offenders as constituting less of a risk for punishment. Cherbonneau and Copes (2006) similarly conclude, based on their study of auto thieves, that using restrictive deterrent strategies may in fact lead to persistence in offending as the offender feels more confident in committing crimes with a (perceived) lower chance of arrest.

Other ethnographic work similarly suggests that restrictive deterrent effects may not necessarily translate into reduced frequency of offending, but may alter offenders' behavior during criminal commission as they attempt to avoid detection and arrest. For example, Wright and Decker (1994) found that the threat of legal sanction did not prevent

burglars from committing an offense but reduced the amount of time they spent committing the crime, while Gallupe et al. (2011) found that some drug offenders switched the location of their transactions or the drug-type sold in response to arrest – although this did not necessarily constitute a reduction in the severity of the offense (see also Jacobs and Cherbonneau, 2012).

Jacobs (2010) ultimately draws the various threads of the literature together and delineates four ways in which restrictive deterrence may affect criminal behavior: First, where the offender reduces offending frequency (as suggested by Gibbs, 1975); second, where the offender commits acts of reduced severity in order to minimize punishment severity; third, where the offender engages in situational measures to try and avoid detection or arrest; and fourth, where the offender displaces their activity to another time or place. Particularistic restrictive deterrent responses may thus variously have the effect of reducing criminal activity; of affecting not its volume or frequency but its location or severity; or indeed of increasing its volume or frequency, depending on the type of response envisaged.

For the purposes of the current study, the first of Jacobs' (2010) restrictive deterrence techniques is the most relevant, inasmuch as the present work examines the post-compromise behavior of attackers with attention to the amount and frequency of the commands they enter on the system. One might suspect that some of the commands entered by attackers may be motivated by a desire to avoid detection in line with Jacobs' (2010) third type of particularistic restrictive deterrent response, and that this may in fact result in an increase of certain commands entered onto the system as the trespasser takes extra measures to scout for potential detectors or to conceal his/her own activity.

However, without access to the attacker's mind one cannot tell whether, for example, the use of a command to edit the timestamp on a file is done with malicious intent or as a means to conceal the attacker's activity and avoid detection. To avoid such speculation, the present work focuses on assessing restrictive deterrence inasmuch as it brings about a reduction in offending, whether because of a probabilistic calculation of long-term odds or a desire to evade detection by limiting illegal activity on systems identified as 'high-risk' by trespassers, in line with Jacobs' (1993) work on particularistic restrictive deterrence. The majority of the work on both probabilistic and particularistic restrictive deterrence supports this expectation of a perceived reduction in offending activity in response to a sanction threat, at least on the monitored system (there is no way to measure its displacement to other systems in line with Jacobs' (2010) fourth particularistic restrictive deterrence response, for example).

Most of the work discussing restrictive deterrence is qualitative in nature and utilizes relatively small samples (Beauregard and Bouchard, 2010; Jacobs, 1993, 1996a, 1996b; Jacobs and Cherbonneau, 2012). The present work, by contrast, offers some empirical analysis of restrictive deterrent techniques, particularly as they result from specific situational cues - for the present study, in the form of warning messages.

2.4 Warning Messages and Deterrence

Geerken and Gove emphasize the importance of regarding deterrence not just as a perceptual process inside the mind of the individual, but as a "mechanism of information transmission" between the sanctioning agent and the individual (Geerken and Gove, 1975:498). Indeed "[t]he success of any deterrence process will be determined by the

degree to which this message is successfully transmitted to the population of potential offenders" (Geerken and Gove, 1975:499). While this may be overstating the matter somewhat, since sanctions will have a differential effect dependent on the characteristics of each individual and their level of 'deterrability' (Geerken and Gove, 1975; Pogarsky, 2002), it is certainly true that in order for legal sanctions to have any deterrent effect, its presence must be communicated to the population of would-be offenders. It is unfortunate, therefore, that the perceptions of sanction severity and certainty held by the general public (and the offender population) are often wildly inaccurate (Kleck et al., 2005). However the use of warning messages provides an opportunity to both inform a potential offender of the presence of a legal sanction, and even to transmit information regarding the certainty and/or severity of that punishment, dependent upon the wording of the message.

There has been considerable work assessing the effectiveness of warning messages on criminal and deviant incidents in the physical world, with mixed results (Borland, 1997; Janis and Feisbach, 1953; Schwartz and Orleans, 1967; Schultz and Tabanico, 2009; Slemerd et al. 2001). In some cases the presence of warnings has been found to increase the non-conformist behavior, which has been variously attributed to the "forbidden fruit" effect, whereby moral injunctions about the inappropriateness of certain behaviors perversely make those behaviors seem more appealing (Grabosky, 1996; Zimring and Hawkins, 1973) and the "advertising" or promotion of that behavior by its mere mention, creating a 'descriptive norm' which encourages individuals to adopt the behavior regardless of the 'injunctive norm' prohibiting it (Cialdani, 1990, 2003; Grabosky, 1996; Keizer et al. 2008).

However most of the work on the deterrent effect of warnings has focused on an investigation of their absolute deterrent effects, with little consideration of any restrictive deterrent effects such as duration of offence or the specific actions committed (although see Maimon et al., 2014). Additionally, despite the prevalence of online sanction threats, little work has addressed cyber-deterrence at all, let alone the specific impact of warning messages in cyberspace.

A considerable body of work has compared the efficacy of sanction threats with that of messages intending to employ techniques of moral persuasion, predominantly with respect to tax law compliance and student cheating. The findings have been somewhat mixed, with some (Schwartz and Orleans, 1967) finding evidence that moral persuasions are more effective at reducing deviant behavior than sanction threats, and others finding the opposite (Tittle and Rowe, 1973). Meanwhile Paternoster and Simpson (1996) concluded that a combination of sanction threat and moral persuasion was necessary to encourage compliance; however Ariel (2010) found no effect of either on tax compliance.

2.5 Deterrence in Cyberspace

Previous empirical work on deterrence in cyberspace is almost non-existent (although for a recent exception see Maimon et al., 2014). There has been, however, a considerable body of work in the realm of cyberdefense investigating the potential for deterrent strategies involving denial of attack by preventing an attack or rendering it futile, and penalty (including the threat of retaliation) (Goodman, 2010). This work emphasizes the importance of credibility – the would-be deterrer must have both the capacity and the intent to enforce penalties in order for them to act as an effective

deterrent (Goodman, 2010). Whether it concerns nation against nation or an individual hacker against another individual's system, the main problem associated with a cyber deterrence strategy is that of credibility, given the lack of capability and intent demonstrated by the legal system when it comes to tackling (especially small-scale) cybercrime. First, it would seem that the legality of system trespassing and related acts, and their associated penalties in criminal law are not necessarily particularly well-known among the general public or the hacking community (see, for example, Furnell, 2002). This constitutes a problem for deterrence, given that it is premised upon the individual knowing their act is punishable by law (Beccaria, 1963 [1764]). Second, youth surveys reveal that even those who know of the illegality of their actions do not seem deterred, since a significant number of young people participate in various computer-related offences and that there is little stigma attached to cybercrime (Choi, 2010; Taylor, 1999; Yar, 2005).

Harknett (1996) states that "[d]eterrence weakens to the degree that the deterrent capability can be contested through degradation or avoidance", and perhaps the greatest problem for cyber-deterrence is that the inherently anonymous nature of cyberspace drastically increases the ability of individuals to avoid detection. Many attacks will go undetected even by the victim; 'policing', such as it exists in cyberspace, is minimal, and formal criminal justice agents lack the resources and knowledge to effectively regulate cyberspace (Choi, 2010). The credibility of legal responses to cyber threats is undercut both by the relative scarcity of prosecutions brought against cybercrime, and (with the exception of a couple of high-profile cases) by the reluctance of the criminal justice system to invoke legal provisions to their full extent when individuals are prosecuted

(Chiesa et al., 2009; Yar, 2006). Hackers themselves do not tend to think their governments take their actions seriously (Chiesa et al., 2009). Additionally, hackers are able to disguise not only their identity but their location through the use of techniques such as "looping", whereby they use one computer system to access another, and then that to access another, and so on. Especially where this crosses national boundaries, it makes it difficult if not impossible to locate where an attack originated (Denning and Baugh, 2000).

However cyber deterrence is not necessarily a 'lost cause'. There has been some argument that it is not necessary to identify specific individuals for deterrence to take effect (Goodman, 2010), and hackers have generally been presumed to demonstrate rational decision-making, evidenced by their actions. Once they have entered a system, hackers may first try to erase the record of their intrusion and then build a 'backdoor' into the system so they can exit and re-enter the system at will (Chiesa et al., 2009; Wang, 2003). Their attempts to avoid detection suggest a mindfulness of the need to employ restrictive deterrence tactics similar to those described by Jacobs in his work on drug dealers (Gibbs, 1975; Jacobs, 1993, 1996a, 1996b) and the 'forensic awareness' techniques utilized by street criminals (Beauregard and Bouchard, 2010). Hackers may, therefore, be responsive to some deterrence strategies, particularly when reminded of the illegality of their actions and the potential consequences by a warning message. Further evidence in support of this conclusion has been offered by Maimon et al.'s (2014) study of the effect of a single warning banner on system trespasser behavior, where it was found that although the banner did not lead to immediate termination of a session or a reduction in the frequency of trespassing incidents, the duration of such incidents was

reduced. This is consistent with the work of Wright and Decker (1994) on restrictive deterrence in the context of burglary. The present study goes beyond Maimon et al.'s (2014) work to examine both the effects of multiple warning messages, and the details of system trespasser behavior once the system has been accessed.

3. THE PRESENT STUDY

Before logging onto computers on university and governmental networks, a banner is often displayed detailing the terms of access and penalties for improper use (NIST 2009). Given the wide use of such banners there appears to be an implicit assumption that these methods of deterrence will be effective in reducing criminal computer activity, but the veracity of this assumption and the extent of the deterrent effect of such warnings have only recently started to undergo theoretical testing (see Maimon et al., 2014 for perhaps the first such work). The present study seeks to empirically test the effectiveness of different warning banner content in mitigating system trespassing events. Specifically, I explore whether a threatening warning banner is more effective in deterring system trespassers behaviors on the system in comparison to banners attempting to reduce crime by moral persuasion, and banners that carry an ambiguous threat. Since one cannot know the thought process or circumstances of individual system trespassers, who might be located anywhere in the world, one cannot claim that system trespassers immediately leaving the system after encountering a warning banner constitutes absolute deterrence. Although measuring absolute deterrence is difficult, it is possible to identify and investigate the use of techniques of restrictive

deterrence, as described by Gibbs (1975) and Jacobs (1993, 1996a, 1996b, 2010), across the experimental and control conditions.

3.1 Research Hypotheses

Restrictive deterrent techniques in the context of system trespassing can be conceptualized as resulting from both probabilistic and particularistic restrictive deterrence (Jacobs 1996a). Probabilistic restrictive deterrence should encourage a limiting of the frequency of criminal behavior in order to (it is assumed) reduce the likelihood of detection or arrest over the long-term. Thus it might be expected that the presence of a warning banner will cause a decrease in the frequency of commands used as the individual seeks to avoid detection. There are some arguments from particularistic restrictive deterrence that suggest that this is not necessarily the case, and that there may be an increase in at least some commands as the individual attempts to conceal their activity (see for example Cherbonneau and Copes, 2006). However none of the commands considered here are solely designed for the purposes of avoiding detection – they all have multiple functions, and ultimately all are being used to effect changes or conduct activities illegally on a trespassed system. They are thus all examples of criminal behavior, whatever their intended function. Therefore I concentrate on the expected restrictive deterrent effect that all command usage should decrease when confronted with a warning message in order to reduce the odds of detection. Whether this is because of a probabilistic restrictive deterrence response concerned with long-term odds of detection, or a particularistic restrictive deterrence response concerned with evading detection in the short-term by reducing activity on systems identified as ‘high-risk’, as in Jacobs’ (1993,

see also Gibbs, 1975; Jacobs, 1996a) work on drug dealers, cannot be stated with certainty, but the observed results will be the same.

There is no clear consensus in the theory as to whether a legal sanction threat, moral persuasion or an ambiguous threat would have a greater deterrent effect. This is in part due to conflicting findings when experiments comparing the effectiveness of legal sanctions and moral persuasion on compliance have been conducted (Ariel, 2010; Paternoster and Simpson, 1996; Schwartz and Orleans, 1967; Tittle and Rowe, 1973) and in part because these three conditions have not, to this writer's knowledge, been considered in relation to each other before. However one might expect, given both extant theory and previous findings, that a legal sanction threat will increase the use of restrictive deterrence techniques (see for example Gallupe et al., 2011; Jacobs, 1993, 1996a, 1996b; Johnson and Natarajan, 1995; VanNostrand and Tewksbury, 1999; Maimon et al, 2014) and so will work to reduce the incidence of criminal and malicious activity over time, although (as noted above) there is some conflicting evidence from research on particularistic restrictive deterrence on this point (see for example Cherbonneau and Copes, 2006). Therefore, I hypothesize that:

Hypothesis 1: A standard legal warning will be associated with a decreased use of commands designed to change aspects of the trespassed system, to scout the system and to bring files from remote networks onto the system. This decrease in command usage will occur as part of a restrictive deterrent response designed to limit the chances of detection while on the system.

Some research suggests that moral persuasion may be effective in reducing the occurrence of criminal activity (Clarke 1996; Paternoster and Simpson, 1996: Schwartz and Orleans, 1967, although see Ariel, 2010; Tittle and Rowe, 1973), and therefore we may tentatively form the following hypothesis:

Hypothesis 2: A moral persuasion message will be associated with a decreased use of commands designed to change aspects of the trespassed system, to scout the system and to bring files from remote networks onto the system.

The literature on ambiguity in threats suggests that raising the ambiguity of the certainty of low-certainty threats increases the perceived certainty (Kahneman and Tversky, 1979; Loughran et al., 2011). Following deterrence theory, this would also increase deterrence. Given that the objective certainty of punishment for computer crime is very low, and there is little expectation of punishment (Choi, 2010; Chiesa et al., 2009; Yar 2006), it may be assumed that any ambiguity in a warning message related to system trespassing will serve to overweight the perceived probability of detection, and that this may lead to deterrence. There is little if any literature explicitly discussing the deterrent effect of ambiguity of perceived sanction severity in isolation from perceived certainty, but one might assume that the potential for any of a number of unspecified punishments not merely limited to legal penalties might increase the deterrent effect of a warning message. Therefore, the findings here suggest that an ambiguous threat message will reduce the occurrence of criminal activity:

Hypothesis 3: An ambiguous threat message will be associated with a decrease in the use of commands designed to change aspects of the trespassed system, to scout the system and to bring files from remote networks onto the system. This decrease in command usage will occur as part of a restrictive deterrent response designed to limit the chances of detection while on the system.

Finally, since the perceived certainty and severity may be heightened for the ambiguous threat message as compared to the standard legal sanction message due to the way in which the human brain processes ambiguity in the assessment of risk and penalty (as suggested by Kahneman and Tversky, 1979; Casey and Scholz, 1991; Loughran et al., 2011b), one might hypothesize that:

Hypothesis 4: System trespassers confronted with the ambiguous threat message will display a higher rate of use of restrictive deterrence techniques designed to reduce criminal activity, as compared to those trespassers confronted with a standard legal sanction. This will translate into a decrease in the use of commands designed to change aspects of the trespassed system, to scout the system and to bring files from remote networks onto the system.

4. DATA AND METHODS

An experiment was developed based on a pilot experiment conducted by Maimon et al. (2014) which focused on the impact of a single warning message on attackers' post-

compromise behavior. The success of this experiment encouraged an increase both in the scale of the experiment and its reach, with an expansion to non-American computer network infrastructures. The present study utilizes data gathered from a Chinese University computer network, where a network of several hundred high-interaction 'honeypots' (a 'honeynet') was set up.

A honeypot is "a security resource whose value lies in being probed, attacked, or compromised" (Spitzner, 2002). Honeypots typically run on a single computer which mimics the activity of a whole network whilst offering easily exploitable flaws to 'lure' hackers into trespassing (Wang, 2003). As (presumed) rational actors, hackers generally look for the easiest computer to break into and then use that to store incriminating files and to launch attacks on other systems (Wang, 2003), making honeypots attractive targets for them. The honeypots get no legitimate traffic except those users who have entered through brute force attacks, so they are an efficient way of gathering attack data (IEEE Computer Society, 2003; Spitzner, 2003). As compared to a low-interaction honeypot (which tends to be used for production purposes), high-interaction honeypots such as those used in the present study are primarily used for research purposes since they are able to capture extensive information on attacker behavior without making any assumptions about how the attacker will behave (Spitzner, 2003).

While there is a dearth of previous empirical research on deterrence and warning messages in cyberspace, in the past decade there have been a number of studies which utilize honeypots to gather data about attacker behavior after system compromise. These studies have generally modeled attacker behavior after ingress into a system without any warning message and found, contrary to their expectations, that if there is no explicit

sanction threat few hackers engage in behaviors designed to conceal their malicious activity. Alata et al. (2006) find that only 14 of 38 intruders attempted to delete the file containing the history of their commands, and Salles-Lostau et al. (2011) similarly find that while more than 90% of attackers checked the system for the presence of other users and almost 80% changed the account password, less than 60% hid their actions. A study by Berthier et al. (2009) found that while the second most installed software were 'Bouncers' (designed to hide source IP addresses and hostnames by relaying connections), only 26% of sessions contained commands to hide the attacker's intrusion. However most of the sessions were short and lasted less than one minute, and some attackers compulsively using the command *w* to make sure no other legitimate user could connect while they were engaged in their attacks (Berthier et al., 2009). These findings partially support Alata et al.'s (2006) conclusion that most hackers fail to engage in activities to avoid detection, although it would seem that at least some are mindful of the need to employ restrictive deterrence strategies, and that some restrictive deterrence strategies may be more common than others. This relatively low level of mindfulness of the need for strategies to lower the odds of detection in the absence of warning messages is, if anything, fortunate for the present experiment since the fact that hackers do not seem to overwhelmingly engage in acts designed to reduce their chances of detection when faced with a lack of warning messages means that it should be easier to detect any restrictive deterrent effect when warning banners are introduced.

The only previous work to explicitly and empirically investigate the deterrent effect of warnings in cyberspace is that conducted by Maimon et al. (2014). Similar to the present study, their study was set up so that upon unauthorized entry to a honeypot,

system trespassers were randomly assigned to either a warning (treatment) or no-warning (control) computer. They found that while the presence of a warning banner did not seem to be associated with an immediate termination or a reduction in the frequency of trespassing incidents, it did significantly reduce the duration of such incidents. They interpreted their results as suggesting that while warning messages in cyberspace do not seem to have an absolute deterrent effect (inasmuch as they do not seem to prevent criminal activity) they may have a restrictive deterrent effect. The results suggest that trespassers attempt to restrict the time they spend on the system after being confronted by a warning banner in an attempt to minimize their chances of detection and thus penalty.

4.1 Procedures

The present study thus builds on the suppositions of the Maimon et al. (2014) paper in investigating the potential restrictive deterrent effects of warning messages. However, where the Maimon et al. (2014) experiment utilized only one experimental condition (the presence of a warning banner) and one control condition (no message), the present study utilizes three experimental conditions in addition to the control (see Appendix A). To ensure the collection of sufficient data across the four conditions and a randomized experimental design, attackers were randomly assigned to one of the four conditions after successfully breaking into the target computers. Specifically, trespassers were allowed access once they had attempted to 'brute force' an entry (i.e. trying to guess the password by trying multiple possible keys) a predefined number of times. This threshold was randomly set at between 150 and 200 attempts. Once they had accessed the

system computers, all of which ran Linux Ubuntu 9.10 with a modified version of an OpenSSH server, trespassers were randomly assigned to one of the four conditions.

The four conditions consisted of a control condition with no message; an 'altruistic' message aimed at moral persuasion (Warning 1); a legal sanction threat consistent with restrictive deterrent theorization (Warning 2); and a non-specific (ambiguous) threat (Warning 3) (see Appendix A for the content of the warning banners). There is little in the extant literature to inform estimates of the relative efficacy of these three experimental conditions, but the research hypotheses discussed above describe some *a priori* assumptions regarding the expected findings.

Trespassers were then allowed access to the target computer, and able to initiate repeated system trespassing incidents, for a period of 30 days. They were free to use the computer as they liked, but a firewall was employed to ensure that they did not engage in activities dangerous to other systems. Their keystrokes were logged using the Sebek keylogger. At the end of the 30-day period they were blocked from the target computer, it was cleaned and redeployed on the network so that others might access it.

4.2 Data

In total 1,231 sessions were logged across 295 deployments: 325 on the control honeypot (no warning message), 189 on the first experimental condition (altruistic warning message), 344 on the second experimental condition (standard legal warning message) and 373 on the third (ambiguous warning message). Of those sessions, 425 have keystrokes logged: 120 on the control honeypot, 62 on the first experimental condition, 125 on the second condition and 118 on the third condition. We cannot

speculate as to what causes some system trespassers to log onto the system and then fail to use it whilst others enter keystrokes, nor is there any obvious way in which we might obtain the data necessary to make such deductions. Overall there is an average of roughly 4 sessions per honeypot deployment.

[INSERT TABLE 1.]

The present study moves beyond an analysis of attack frequency and duration and builds on the prior work of Ramsbrock et al. (2007) and Berthier et al. (2009) in examining the commands used by attackers confronted with each of the study conditions through analysis of keystroke data. Keystroke data refers to the output data when keystrokes are logged; that is, when the typing activity of individuals on a system is recorded and transcribed. For the present study this logging is carried out covertly, and the end-product is a dataset consisting of a list of all keys typed by individuals as they trespass into the system. From this it is possible to isolate and analyze the commands entered by system trespassers.

Overall, 14 individual commands were examined in the present study. These commands are first studied individually, in order to address the contention that certain commands may be utilized more frequently on systems with warning banners for reasons of particularistic deterrence, while others may be used less frequently for reasons of probabilistic deterrence. The 14 commands are then divided into three categories and analyzed with reference to their general function. Here I follow the example set by previous work on post-system compromise attacker behavior which looks at attacker behavior with reference to the general function of commands (Berthier et al., 2009;

Ramsbrock et al., 2007). Here I investigate whether different forms of hacker engagement with the system may be affected differently by the various warning messages. This is something that has not been considered in the context of deterrence before, however, and so I have no theoretical basis for predicting what differences may occur or for which command groupings. My hypotheses predict, in accordance with most theory on probabilistic and particularistic restrictive deterrence, a decrease in the usage of all commands upon confrontation with a warning, but it is possible that commands displaying certain functions may be reduced more or less severely compared to other types of command. The three categories into which the 14 commands are divided are labeled as Change commands, Reconnaissance commands and Fetch commands. Change commands are those commands that change files, access permissions or processes on the computer. The commands included as such are *adduser*/*useradd*, *passwd*, *chmod*, *rm -rf*, *touch* and *kill*/*killall*. The Reconnaissance commands are designed to report information about the computer's contents and processes. The commands considered here are *w*, *uname*, *ps*, *uptime* and *ls*. The third category of Fetch commands are designed to fetch files from other networks and bring them to the compromised computer. The commands included here are *wget*, *tar* and ftp. Table 2 presents a list of these commands as well as their description.

[INSERT TABLE 2]

4.3 Methods

I ran power analyses to confirm that the sample sizes used were sufficient to correctly reject the null hypothesis when it is false, i.e. that my sample was large enough

that it would be able to find significant differences should they exist and calculate a sufficiently accurate estimate of the effect sizes for any significant differences. For this I used the power analysis software G*Power. The current data has enough power at the generally accepted standard of $\pi = 0.80$ to detect a medium effect size of r = 0.25 at an alpha level of 0.05, which is the accepted significance level. I should therefore be able to detect and measure with sufficient accuracy falsifications of the null hypothesis and significant findings in my data analysis.

To analyze the data, I first created a 'proportion' measure for each individual command which represents the proportion of honeypots deployed upon which that individual command had been logged one or more times. This was to allow comparison across treatment conditions of the proportion of honeypots logging commands as compared to those where the command was not logged at all. I then created a second 'rate' measure for each individual command which represents the rate at which those commands were entered on each deployment. On average the number of system trespassing incidents per deployment was roughly 4 (see Table 1.), but when I used this to create rates of command usage per individual deployment the resulting rates were very low (several decimal places past zero) and thus I instead created a command usage rate per 10 trespassing incidents. I then created new rate measures for the three command categories discussed above (Change, Reconnaissance and Fetch) by combining the rates of usage of the individual commands in each category. These rates are also calculated per 10 trespassing incidents.

Due to the set-up of this experiment, there are no additional variables that must be controlled for, nor is there any sample selection bias. The collected data may thus be

analyzed without the use of statistical regression. Instead, I use several statistical methods designed to find significant differences across treatment conditions and between paired conditions – that is, to find differences which are highly unlikely to be coincidental, and thus which indicate some effect of the presence of a warning message on system trespasser command use.

I analyzed the proportion data using a chi-squared test. The chi-squared test examines 'goodness of fit', that is, how closely observed data conforms to the data we would expect from a population with a normal distribution, and then tests for significant differences if the observed and expected data are at variance. Here, if there were no effect of any warning banner, we would expect to see no difference in the proportion of honeypots registering command use across treatment conditions. Where a significant difference is shown, we can conclude that there is only a 5% or 10% probability (depending upon our chosen level of significance) that this finding is due to chance, and therefore that the difference is a result of the presence of a warning message.

I analyzed the rates first using one-way ANOVA. One-way analysis of variance compares the means across samples using the F distribution, and finds significant differences between those means by testing whether the samples seem to be drawn from populations with the same mean values. Where means are found to be significantly different, this suggests that the samples do not come from similar populations. Given that treatment conditions are randomly assigned, the population of system trespassers itself should exhibit no significant or systematic differences across treatment conditions prior to the introduction of a warning message. Thus our null hypothesis for the purposes of one-way ANOVA testing is that the population across samples should exhibit the same

mean, unless warning messages have an effect. If we do see significant differences, therefore, we can conclude with a high probability that warning messages bring about a change in attacker behavior (specifically, here, a change in the frequency of command usage). I also ran Tukey's test on each command to find if the means for each treatment condition were significantly different to each other. This method is more suited to the present study than simple t-testing, since it is more conservative when there are unequal sample sizes, as there are in the present study due to the lower number of system trespassing incidents registered for the first treatment condition (the altruistic warning message). Tukey's test gives an idea of whether there is a significant difference in the rate of commands logged across honeypot type by comparing each possible set of paired conditions. Where a pair registers a significant difference, it can be concluded to the appropriate degree of probability that those two conditions come from populations with different means – i.e., populations that are substantially different to each other. Given the nature of the current experiment, that difference can only come from the effect of the warning message.

I then ran both one-way ANOVA and Tukey's tests for the Change (*adduser*/*useradd*, *passwd*, *chmod*, *rm -rf*, *touch* and *kill*/*killall*), Reconnaissance (*w*, *uname*, *ps*, *uptime* and *ls*) and Fetch (*wget*, *tar* and *ftp*) grouping rates. This was to see if there were significant differences first in the frequency of command usage between all condition types and then between each set of pairs for these three general types of attacker behavior.

5. RESULTS

I look first at the proportion of honeypot deployments in which each command is used, and then compare these proportions by treatment condition. Table 3 shows the proportion of all honeypots deployed where a command was logged. This data alone does not tell us how many times a command was used on each honeypot, but demonstrates the relative number of honeypots that logged a certain command in comparison to those which never logged that command. This data allows one to determine which warning messages affect whether or not a command is used at all. Chi-squared testing reveals two significant findings. There are significant differences between the three treatment groups and the control for the proportion of honeypots logging the command *rm –rf*, at a significance level of $p < 0.05$, and for the command *chmod* at a one-tailed significance level of $p < 0.05$. *Rm –rf* is a command that functions as a delete-all, and is used to remove files and directories. The *chmod* command changes the access permissions for files, allowing intruders to read and edit previously restricted files. Both commands thus wreak changes upon the computer system and are classified as 'Change' commands. It is possible that they may be used in a malicious manner, to edit or delete files on the original system, but one can only speculate as to the intentions behind the use of these commands. In both cases a far lower proportion of the altruistic than the ambiguous honeypots log the command. Indeed a general pattern is quite striking when one looks at the data in Table 3. Although there are no further significant differences, for most commands (11 out of 14) altruistic honeypots register a lower proportion of command usage than the other three conditions, which are generally largely similar to each other. For instance, the command *ps*, which is a 'Reconnaissance' command that reports on current processes, is used on 18.97% of altruistic honeypots but on between 25.64% and

29.63% of honeypots for the other three conditions, despite statistical testing finding no significant difference across conditions.

[INSERT TABLE 3.]

The proportion of honeypots logging each command only gives us part of the picture, however. It is also important to consider how many times the command was used on each honeypot, in order to assess whether command usage was truly higher or lower across treatment conditions. On average each deployment consisted of 4.17 trespassing incidents, but in order to make the data more amenable to visual analysis the rate of command use was calculated for 10 sessions. One-way ANOVA analysis of the differences between all condition types reveals significant differences in the rates of usage of the *chmod* command at a one-tailed level of $p < 0.05$. Tukey's test finds that for *chmod* there is a significant difference between the altruistic message and the ambiguous warning at a one-tailed level of $p < 0.05$. Again, most of the commands (11 out of 14) show a non-significant lower rate of command usage for the altruistic message condition as compared to the other three conditions. There is therefore a clear pattern that the moral persuasion message is working to reduce both the incidence and the frequency of most commands, albeit mostly at non-significant levels. The three commands for which the altruistic condition does not log the lowest proportion of commands are *adduser*, *passwd* and *wget*, whilst the three commands for which the altruistic condition does not record the lowest rate of occurrence are *adduser*, *wget* and *tar*. Looking at the function of these commands as compared to the other commands studied (see Table 2.) there is no obvious theoretical reason why they should be higher for the altruistic condition. Given that there

is no significant difference for either proportion or rate for any of these commands, it seems likely that their higher incidence is merely coincidental.

[INSERT TABLE 4.]

Finally I looked to see if there were differences in the rate of usage of commands as divided into three categories with reference to their function. While I predicted that all three categories would experience a reduction on the treated honeypots, I followed the example of previous work on system trespasser behavior (albeit simplified for the present study in recognition of the smaller sample size and reduced number of commands studied) in looking at the various ways an attacker might engage with the system – through changing aspects of the system (Change), through the use of commands designed to gain information about the system and its processes (Reconnaissance), and by bringing files from remote networks onto the hacked system (Fetch) (see Berthier et al., 2009; Ramsbrock et al., 2007). Neither the Fetch nor Reconnaissance groupings demonstrated any significant differences across treatment conditions, but the Change grouping showed a difference across condition types at a one-tailed significance level of $p < 0.05$ under one-way ANOVA testing, while Tukey's test revealed a difference between the altruistic and the ambiguous warning at a one-tailed significance level of $p < 0.05$. It is likely that this finding of significance is driven by the fact that the Change group includes the two commands that yield significant differences on their own – the *chmod* and *rm –rf* commands. Yet the findings suggest that while there is no significant difference in reconnaissance activities or those directed towards bringing files onto the system from remote networks, tampering with data and access permissions within the computer is

lessened by the presence of the moral persuasion message, especially as compared to an ambiguous threatening message.

[INSERT TABLE 5.]

6. DISCUSSION AND CONCLUSIONS

6.1 Discussion

System trespassing, or the unauthorized entry of individuals into a computer system, is one of the many forms of cybercrime that has become a growing concern with the spread of computer technologies worldwide (Bursztein, 2013; Hernandez-Castro and Boiten, 2013). Yet this area has remained largely unexamined within the context of criminology, despite offering a novel arena in which to test established criminological theory. The present study is among the first (see also Maimon et al., 2014) to apply deterrence theory to the realm of cyberspace. The experiment conducted seeks to establish the restrictive deterrent effect of textual computer warnings on the behavior of system trespassers once they have entered a computer system. The focus is on the restrictive deterrence identified by Gibbs (1975) and refined by Jacobs (1993, 1996a), examining whether the presence of a warning message causes a decrease in the number of commands entered after system entry in an attempt to limit the chances of detection. By utilizing not a single warning message but three messages which comprise a 'generic' legal sanction threat, a moral persuasion message and an ambiguous warning, the present study seeks to establish not only whether the presence of a warning message matters, but whether the type of message makes a difference to attacker behavior. The conclusion that can be reached is that the type of message does indeed matter, with some substantial

evidence indicating that while we do not find the predicted restrictive deterrent effect for the legal sanction threat or the ambiguous warning, we do find a reduction in attacker activity for the moral persuasion message, in line with some (albeit not all) of the previous research comparing the effects of moral persuasion and legal warnings (Paternoster and Simpson, 1996; Schwartz and Orleans, 1967; although see Ariel, 2010; Tittle and Rowe, 1973).

The hypothesis for which I find the greatest evidence is Hypothesis 2 – that a message of moral persuasion will cause a decrease in the commands used by a system trespasser on a compromised computer system. There is evidence of significant reductions in command usage for two commands – *chmod* and *rm –rf* – as well as for the 'Change' category within which these commands fall. Overall there is also an insignificant but clear pattern of lower command usage on the 'altruistic' condition honeypots. This holds true for both the proportion of honeypots registering commands and for the frequency of command usage. There is thus some substantial evidence that the presence of a moral persuasion message causes system trespassers to reduce their criminal activity on the system, in line with some of the findings testing the efficacy of moral persuasion in reducing the occurrence of other forms of criminal activity, such as tax evasion (see for example Paternoster and Simpson, 1996; Schwartz and Orleans, 1967). The reduction in activity for the Change command grouping as opposed to the Reconnaissance or Fetch groupings suggests that it is primarily that activity where trespassers alter (or damage) the system which is reduced by the presence of a moral persuasion message. Reconnaissance activity which merely reports on system processes (and is therefore less 'intrusive') is not affected, but neither is 'Fetch' activity which

involves the bringing of files into the network. One might expect Fetch to be affected in a similar manner to Change, given that it also alters the contents of the computer system, and why the one is affected but not the other is unclear. It may be that a dataset with a higher power might identify differences that cannot be detected in the present data, or that an investigation of the contents of the files imported by Fetch commands might explain the different behavior of the Fetch and Change categories.

There is considerably less evidence in favor of Hypotheses 2 and 3, however. No significant differences are found between the proportion or rates of commands on the second and third treatment conditions as compared to the control condition, and in fact there is a mild suggestion of a pattern favoring a higher proportion and rate of command usage on the two treatment conditions (especially condition 3), in contradiction of my prediction. For 9 out of the 14 commands a higher proportion of legal standard honeypots registered a command usage as compared to the control, whilst ambiguous honeypots registered higher for 13 out of 14 commands. The legal standard honeypot type registered a higher rate of use than the control condition for 8 out of 14 commands, whilst the ambiguous warning registered a higher rate for 12 out of 14. It is unclear why the two conditions suggest higher rates of criminal activity than the control, and it may be that trespassers on those two conditions are in fact increasing their use of commands designed to conceal their activity and their presence on the system, similar to the form of particularistic restrictive deterrent response described by Cherbonneau and Copes (2006) where there is not necessarily a reduction in criminal activity (and there may in fact be a increase) because of the attacker's response to a legal sanction threat (see also Gallupe et al., 2011; Wright and Decker, 1994). In the context of the present study, however, the

commands alone do not allow us to conclude whether or not system trespassers are acting with such an intention. Given the insignificant nature of the findings regarding the legal sanction threat and the ambiguous warning, one can only conclude that no restrictive deterrence seems to be taking place.

There is some, again insignificant evidence that suggests a difference between the generic legal warning and the ambiguous warning, although in the opposite direction from that predicted in Hypothesis 4. The data in Tables 3 and 4 show that a higher proportion of ambiguous honeypots log commands for 10 out of the 14 commands, and that there is a higher rate of command entry on the ambiguous honeypots for 8 out of the 14 commands. We thus see a greater increase of command usage relative to the control condition for the ambiguous honeypot type, perhaps in line with a particularistic deterrent approach encouraging an increase in commands designed to shield the attacker from detection, although again that is mere speculation. The relative similarity of the data for the control condition and the generic legal warning may be explained by system trespassers failing to read, or even take much notice of the legal warning, as opposed to the other two warnings. Anyone who spends much time on the internet will encounter similarly structured and worded warnings frequently (when logging on to restricted access systems in universities or workplaces, signing up for accounts with social networking sites such as Facebook or joining public wifi services in establishments such as Starbucks) and these warnings tend to have a generic layout and content. It may be, then, that people do not bother to read the legal warning, since they assume that they know its contents already and are used to encountering and disregarding such messages with some considerable frequency. If people fail to read the legal warning, it will operate

much like the control condition (that is, as if there were no warning at all). By contrast, the altruistic warning and ambiguous warning, due to their different layout and content, are less likely to be immediately dismissed by trespassers. System trespassers may be more likely to read these messages, and thus they are able to influence behavior, in whatever form that may take. This may be why we see a greater difference with comparison to the control condition for both the proportion and rates of command usage for these two conditions. Again, however, the differences for all but the altruistic warning are insignificant and may be a result of coincidence, so no hard conclusions can be drawn.

6.2 Conclusions

Whilst most findings fail to reach the commonly accepted level of significance, the results which do meet this level of significance, in addition to the general patterns visible in the data (despite not proving significant under statistical testing), are quite strongly suggestive that a moral persuasion message affects computer system trespasser behavior. The data suggest quite strongly that the altruistic honeypot condition is associated with a lower rate of command usage across all commands, with moral persuasion having a greater impact on reducing both the incidence and the frequency of system trespasser behavior than the other warning message types. Indeed if anything the presence of a legal warning or an ambiguous threatening message seems to increase command usage, perhaps in line with the potential particularistic restrictive deterrence response identified by Cherbonneau and Copes (2006) amongst others, although none of these findings were significant so strong conclusions cannot be formed and it is not

possible to test for a particularistic restrictive deterrent effect with the current data. Generally the results of this study, although not strongly conclusive, suggest that restrictive deterrence does not occur in response to legal threats in cyberspace, perhaps due to the low perceived certainty and severity of punishment (Chiesa et al., 2009; Choi, 2010; Taylor, 1999; Yar, 2006). There is, however, an effect of moral persuasion in reducing criminal activity, and this indicates potential avenues for future study of the ways in which moral persuasion may be employed to reduce (cyber)crime and the methods by which it accomplishes this.

Future study of the effect of moral persuasion (and legal threat) on cybercrime is important not just for theory but for policy. It is important to know what effect different types of warning messages have on system trespasser behavior in order that system administrators can learn how to protect their systems (and the data contained therein) to the best of their ability. The present study suggests that the primary approach to deterring system trespassers or others who would abuse computer privileges - use of a threat of legal sanction – is not only ineffective in reducing criminal behavior but may in fact increase it, or (in line with some forms of a particularistic restrictive deterrent response) encourage criminals to employ commands that make their activity and presence harder to detect. By contrast, a message which appeals to the moral sensibilities of system trespassers has a higher success rate in reducing the activity of trespassers on computer systems, and may be a more effective method of ensuring system safety. In the present study, the two commands which were logged much less often and less frequently for the altruistic condition are both potentially damaging commands from the point of view of a system administrator – *chmod* changes access permissions and *rm –rf* is a delete-all for

files and directories. Reducing the incidence of these commands amongst others during a trespass incident is certainly in the interests of a system administrator. The present study thus has important ramifications for policy approaches, inasmuch as it suggests practical methods by which unwanted system activity may be reduced and computer network safety increased.

6.3 Limitations and Future Directions

The present study represents a first move towards addressing an important and understudied issue: that is, how effective are computer warnings at preventing unlawful system access? The present study looks specifically at the effect of various warning messages on system trespassing activity. The tendency for system administrators, websites and online service providers to use textual warnings to try and discourage either system trespassing or abuse of system privileges seems to be based on an assumption that deterrent principles are effective, yet this has rarely been tested in practice. Given the desire of system administrators to protect their systems, it is important to know whether or not warning messages are effective, and which type are most effective, in encouraging individuals to restrain their criminal activity. It is also important to know whether warning messages encourage system trespassers to conceal their activity, because this will make them potentially more difficult to detect. Therefore experiments such as the one discussed in the present work are important in practical terms for suggesting ways in which systems may be made safer and the data on them protected more effectively.

The present study is limited in its conclusions partly by the paucity of significant findings. It may be that a study on a larger scale will find more clearly defined patterns in

the data that can corroborate the conclusions tentatively drawn here. The current sample size was only large enough to find moderate effects with an effect size of 0.25. Additionally, there are some commands that may be used frequently enough in a larger study to warrant inclusion in the analysis which may shed more light on the ways in which differing treatment conditions affect the usage of different commands. These commands may make it easier to isolate any particularistic restrictive deterrence responses which may take the form, as suggested by Cherbonneau and Copes amongst others (Cherbonneau and Copes, 2006; see also Gallupe et al., 2011; Wright and Decker, 1994), of attempts to avoid detection through the usage of commands for that purpose. This type of particularistic restrictive deterrence approach might in fact yield an increase in command usage as the attacker seeks to reduce their chances of detection by using commands to conceal their presence, in line with the third type of particularistic restrictive deterrent response identified by Jacobs (2010). This constitutes the opposite of the effect of either a probabilistic restrictive deterrence response or the particularistic restrictive deterrence response first identified by Gibbs (1975) and given by Jacobs as the first type of particularistic restrictive deterrent response in his 2010 typology. In the present study, it was not possible to isolate this potential effect (although there was little solid evidence of one) since the intent of the system trespasser in using any of the commands studied could not be known. This is a problem that future work should attempt to address, perhaps through ethnographic work on self-identified system trespassers similar to that conducted by Jacobs on drug dealers where this type of potential restrictive deterrent effect was first identified (1993, 1996a).

A further limitation is that the results of the present study are applicable only to a subset of system trespassers – likely the less skilled or purposeful hackers, who select targets for intrusion based on port-scanning techniques that locate easy targets. It is debatable whether system trespassers who consciously select their targets and enter them using a high degree of skill in order to access specific information would be affected by warning messages in the same way (if at all). It is unclear how many system trespassers fall into the first camp (unskilled and selecting targets at random) as opposed to the second (skilled and goal-focused), although logically one might suppose there are more in the former than the latter. Research on the proportion of system trespassers who consciously target specific systems as opposed to targeting easily-accessed systems at random would inform the applicability of the present study's findings.

In general, however, the present study constitutes one of the first attempts to apply deterrence theory to the cyber realm. The findings are preliminary, but suggest some directions for future research in investigating the relative effect of attempts at moral persuasion and legal sanction threats in reducing the criminal behavior of trespassers on computer systems. It is hoped that such research will inform the decisions of system administrators in their mission to maintain the safety of their networks and the protection of the data housed therein.

7. TABLES

TABLE 1. Descriptive Statistics: Honeypot Deployments and Sessions

Condition	No. of deployments	No. of trespassing incidents	Mean no. of trespassing incidents per deployment	No. of trepassing incidents with keystrokes
Control	78	325	4.17	120
Altruistic Warning	58	189	3.25	62
Legal Warning	78	344	4.41	125
Ambiguous Warning	81	373	4.60	118
Total	295	1231	4.17	425

TABLE 2. Command List

Command	Description of Command
w	Shows whether other users are logged into the system and their activity
uname	Reports basic information about the computer's hardware and software
uptime	Shows whether other users are logged on and how long the system has been running
ps	Reports on current processes
adduser / useradd	Creates a new user account
passwd	Changes the password
chmod	Changes access permissions
rm -rf	Functions as a delete-all
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
ls	Lists all files

TABLE 3. Proportion (as a percentage) of deployments where a command was used one or more times

Command Name	All Honeypot Types	Control	Altruistic Warning	Legal Warning	Ambiguous Warning
w	40.34	39.74	36.21	41.03	43.21
uname	18.64	17.95	12.07	20.51	22.22
uptime	4.41	5.13	1.72	6.41	3.70
ps	25.76	26.92	18.97	25.64	29.63
adduser	2.37	1.28	1.72	2.56	3.70
passwd	42.03	42.31	37.93	37.18	49.38
chmod *	16.61	12.82	8.62	19.23	23.46
*rm –rf***	20	19.23	8.62	19.23	29.63
touch	2.37	2.56	1.72	2.56	2.47
kill	11.53	10.26	8.62	11.54	14.81
wget	25.08	23.08	27.59	24.36	25.93
tar	15.93	15.38	12.07	12.82	22.22
ftp	3.73	2.56	1.72	5.13	4.94
ls	29.15	25.64	20.69	34.62	33.33

* Chi-squared test is significant at a one-tailed level of $p<0.05$.

** Chi-squared test is significant at a level of $p<0.05$.

TABLE 4. Rate of command usage per 10 sessions

Command Name	All Honeypot Types	Control	Altruistic Warning	Legal Warning	Ambiguous Warning
w	1.66	1.73	1.43	1.72	1.70
uname	0.66	0.52	0.48	0.78	0.82

uptime	0.19	0.26	0.06	0.21	0.21
ps	0.87	1.12	0.61	0.78	0.91
adduser	0.05	0.02	0.04	0.02	0.10
passwd	1.48	1.33	1.31	1.37	1.86
chmod *	0.43	0.38	0.21**	0.37	0.69
rm –rf	0.66	0.74	0.29	0.68	0.84
touch	0.07	0.07	0.02	0.05	0.10
kill	0.26	0.32	0.17	0.27	0.27
wget	1.00	0.90	1.01	1.15	0.94
tar	0.44	0.50	0.32	0.31	0.61
ftp	0.15	0.15	0.09	0.22	0.12
ls	1.14	1.09	0.79	1.43	1.18

* One-way ANOVA test is significant at a one-tailed level of $p<0.05$.

** Tukey's test finds a significant difference between the Altruistic Warning condition and the Ambiguous Warning condition at a one-tailed level of $p<0.05$.

TABLE 5. Rate of command usage per 10 sessions for command groupings Change, Reconnaissance and Fetch

Command Group	All Honeypot Types	Control	Altruistic Warning	Legal Warning	Ambiguous Warning
Change *	2.95	2.87	2.05**	2.76	4.83
Reconnaissance	4.53	4.71	3.37	4.92	4.82
Fetch	1.59	1.55	1.41	1.68	1.67

* One-way ANOVA testing is significant at a one-tailed level of $p<0.05$.

** Tukey's test is significant for a difference between the Altruistic Warning condition and the Ambiguous Warning condition at $p<0.05$ one-tailed.

APPENDIX A. Warning Banners Displayed

Panel A. 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

Panel B. University of Maryland 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.

Panel C. Ambiguous Warning (Treatment 3):

We have acquired your IP address.

Logout now and there will not be any consequences.

REFERENCES

Alata, E., V. Nicomette, M. Kaâniche, M. Dacier and M. Herrb. 2006. Lessons Learned From the Deployment of a High-Interaction Honeypot. *Sixth European Dependable Computing Conference*. [accessed online]

Andenaes, Johannes. 1966. The General Preventive Effects of Punishment. *University of Pennsylvania Law Review* 114(7):949-983.

Andenaes, Johannes. 1974. *Punishment and Deterrence*. Ann Arbor, MI: The University of Michigan Press.

Anderson, Linda S., Theodore G. Chiricos and Gordon P. Waldo. 1977. Formal and Informal Sanctions: A Comparison of Deterrent Effects. *Social Problems* 25(1):103-114.

Anwar, Shamena and Thomas A. Loughran. 2011. Testing a Bayesian Learning Theory of Deterrence Among Serious Juvenile Offenders. *Criminology* 49(3):667-698.

Ariel, Barak. 2012. Deterrence and Moral Persuasion Effects on Corporate Tax Compliance: Findings from a Randomized Controlled Trial. *Criminology* 50(1):27-68.

Beauregard, Eric and Martin Bouchard. 2010. Cleaning Up Your Act: Forensic Awareness as a Detection Avoidance Strategy. *Journal of Criminal Justice* 38:1160-1166.

Beccaria, Cesare. 1963 [1764]. *On Crimes and Punishment*. New York, NY: Macmillan Publishing Company.

Becker, Gary S. 1968. Crime and Punishment: An Economic Approach. *Journal of Political Economy* 76(2):169-217.

Bentham, Jeremy. 1948 [1789]. *An Introduction to the Principles of Morals and Legislation*. New York, NY: Hafner Publishing Company.

Berthier, Robin, Jorge Arjona and Michel Cukier. 2009. Analyzing the Process of Installing Rogue Software. *IEEE* 2009:560-565. [accessed online]

Borland, Ron. 1997. Tobacco Health Warnings and Smoking-Related Cognitions and Behaviours. *Addiction* 92(11):1427-1435.

Bosch-Domènech, Antoni and Joaquim Silvestre. 2006. Reflections on gains and losses: A 2 x 2 x 7 experiment. *Journal of Risk Uncertainty* 33:217-235.

Brenner, Susan W. 2010. *Cybercrime: Criminal Threats from Cyberspace*. Praeger, ABC-CLIO, LLC.

Bursztein, Elie. 2013. *18.4% of US Internet Users Got At Least One of Their Account Compromised*. [accessed online]

Casey, Jeff T. and John T. Scholz. 1991. Beyond Deterrence: Behavioral Decision Theory and Tax Compliance. *Law and Society Review* 25(4):821-843.

Chambliss, William J. 1967. Types of Deviance and the Effectiveness of Legal Sanctions. *Wisconsin Law Review* Summer 1967:703-719.

Cherbonneau, Michael and Heith Copes. 2006. 'Drive It Like You Stole It': Auto Theft and the Illusion of Normalcy. *British Journal of Criminology* 46:193-211.

Cherniak, Christopher. 1986. *Minimal Rationality*. Cambridge, MA: MIT Press.

Chiesa, Raoul, Stefania Ducci and Silvio Ciappi. 2009. *Profiling Hackers: The Science of Criminal Profiling as Applied to the World of Hacking*. Boca Raton, FL: Auerbach Publications.

Choi, Kyung-Shick. 2010. *Risk Factors in Computer-Crime Victimization*. El Paso, TX: LFB Scholarly Publishing.

Choi Kyung-Shick. 2011. Cyber-Routine Activities: Empirical Examination of Online Lifestyle, Digital Guardians, and Computer-Crime Victimization. In *Cyber Criminology*, ed. K. Jaishankar. Boca Raton, FL: CRC Press.

Cialdani, Robert B. 2003. Crafting Normative Messages to Protect the Environment. *Current Directions in Psychological Science* 12:105-109.

Cialdani, Robert B., Raymond R. Reno and Carl A. Kallgren. 1990. A Focus Theory of Normative Conduct: Recycling the Concept of Norms to Reduce Littering in Public Places. *Journal of Personality and Social Psychology* 58(6):1015-1026.

Cohen, Lawrence E. and Marcus Felson. 1979. Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review* 44:588-608.

Denning, Dorothy E. and William E. Baugh. 2000. Hiding Crimes in Cyberspace. In *Cybercrime: Law enforcement, security and surveillance in the information age*, eds. Douglas Thomas and Brian D. Loader. London, UK: Routledge.

Erickson, Maynard L., Jack P. Gibbs and Gary F. Jensen. 1977. The Deterrence Doctrine and the Perceived Certainty of Legal Punishments. *American Sociological Review* 42:305-317.

Furnell, Steven. 2002. *Cybercrime: Vandalizing the Information Society*. Harlow, UK: Pearson Education Limited.

Gallupe, Owen, Martin Bouchard and Jonathan P. Caulkins. 2011. No change is a good change? Restrictive deterrence in illegal drug markets. *Journal of Criminal Justice* 39:81-89.

Geerken, Michael R. and Walter R. Gove. 1975. Deterrence: Some Theoretical Considerations. *Law and Society Review* 9(3):497-513.

Gibbs, Jack P. 1975. *Crime, Punishment and Deterrence*. New York, NY: Elsevier.

Goodman, Will. 2010. Cyber Deterrence: Tougher in Theory Than in Practice? *Strategic Studies Quarterly* Fall:102-135.

Grabosky, Peter N. 1996. Unintended Consequences of Crime Prevention. In *Crime Prevention Studies Volume 5: The Politics and Practice of Situational Crime Prevention*, ed. Ross Homel. New York, NY: Criminal Justice Press.

Harknett, Richard J. 1996. Information Warfare and Deterrence. *Parameters: US Army War College Quarterly* Autumn:93-107.

Hernandez-Castro, Julie and Boiten, Eerke. 2013. *University of Kent Survey on Cyber Security*. [accessed online]

IEEE Computer Society, The. 2003. The Honeynet Project: Trapping the Hackers. *IEEE Security & Privacy* March/April 2003:15-23.

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, Bruce A. 2010. Deterrence and Deterrability. *Criminology* 48(2):417-441.

Jacobs, Bruce A. and Michael Cherbonneau. 2012. Auto Theft and Restrictive Deterrence. *Justice Quarterly* [online]:1-24.

Janis, Irving L. and Seymour Feshbach. 1953. *Journal of Abnormal and Social Psychology* 48(1):78-92.

Johnson, Bruce D. and Mangai Natarajan. 1995. Strategies to Avoid Arrest: Crack Sellers' Response to Intensified Policing. *American Journal of Police* 14(3):49-69.

Kahneman, Daniel and Amos Tversky. 1979. Prospect Theory: An Analysis of Decision Under Risk. *Econometrica* 47(2):263-291.

Keizer, Kees, Siegwart Lindenberg and Linda Steg. 2008. The Spreading of Disorder. *Science* 322:1681-1685.

Kerr, Orin S. 2009. *Computer Crime Law*, 2nd ed. St. Paul, MN: West.

Kim, Helen S. and Michael L. Kamil. 2003. Electronic and Multimedia Documents. In *Rethinking Reading Comprehension* eds. Anne Polselli Sweet and Catherine E. Snow pp.166-175. New York, NY: The Guilford Press.

Kleck, Gary, Brion Sever, Spencer Li and Marc Gertz. 2005. The Missing Link in General Deterrence Research. *Criminology* 43(3):623-659.

Klepper, Steven and Daniel Nagin. 1989. The Deterrent Effect of Perceived Certainty and Severity of Punishment Revisited. *Criminology* 27(4):721-746.

Lee, Cynthia Bailey, Chris Roedel and Elena Silenok. 2003. *Detection and Characterization of Port Scan Attacks*. [accessed online]

Liu, Hsin-Hsien and Andrew M. Colman. 2009. Ambiguity aversion in the long run: Repeated decisions and uncertainty. *Journal of Economic Psychology* 30(3):277-284.

Loader, Brian D. 2000. Introduction. In *Cybercrime: Law enforcement, security and surveillance in the information age*, eds. Douglas Thomas and Brian D. Loader. London, UK: Routledge.

Loughran, Thomas A., Greg Pogarsky, Alex R. Piquero and Raymond Paternoster. 2011a. Re-Examining the Functional Form of the Certainty Effect in Deterrence Theory. *Justice Quarterly* 29(5):712-741.

Loughran, Thomas A., Raymond Paternoster, Alex R. Piquero and Greg Pogarsky. 2011b. On Ambiguity in Perceptions of Risk Implications for Criminal Decision Making and Deterrence. *Criminology* 49(4):1029-1061.

Maimon, David, Mariel Alper, Bertrand Sobesto and Michel Cukier. 2014. Restrictive Deterrent Effects of a Warning Banner in an Attacked Computer System. *Criminology* 52(1):1-27.

Nagin, Daniel S. and Raymond Paternoster. 1993. Enduring Individual Differences and Rational Choice Theories of Crime. *Law & Society Review* 27(3):467-496.

Nagin, Daniel S. and Greg Pogarsky. 2001. Integrating Celerity, Impulsivity, and Extralegal Sanction Threats into a Model of General Deterrence: Theory and Evidence. *Criminology* 39(4):865-890.

National Institute of Standards and Technology. 2009. *Recommended Security Controls for Federal Information Systems and Organizations*. [accessed online]

Paternoster, Raymond. 2010. How Much Do We Really Know About Criminal Deterrence? *Journal of Criminal Law and Criminology* 100(3):765-823.

Paternoster, Raymond. 1987. The Deterrent Effect of the Perceived Certainty and Severity of Punishment: A Review of the Evidence and Issues. *Justice Quarterly* 4(2): 173-217.

Paternoster, Raymond and Alex Piquero. 1995. Reconceptualizing Deterrence: An Empirical Test of Personal and Vicarious Experience. *Journal of Research in Crime and Delinquency* 32(3):251-286.

Paternoster, Raymond and Sally Simpson. 1996. Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime. *Law and Society Review* 30(3):549-584.

Piquero, Alex R. and Greg Pogarsky. 2002. Beyond Stafford and Warr's Reconceptualization of Deterrence: Personal and Vicarious Experiences, Impulsivity and Offending Behavior. *Journal of Research in Crime and Delinquency* 39(2):153-186.

Pogarsky, Greg. 2002. Identifying "Deterrable" Offenders: Implications for Research on Deterrence. *Justice Quarterly* 19(3):432-452.

Pogarsky, Greg, Alex R. Piquero and Ray Paternoster. 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*. [accessed online]

Ramsbrock, Daniel, Robin Berthier and Michel Cukier. 2007. Profiling Attacker Behavior Following SSH Compromises. *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks*. [accessed online]

Salles-Lostau, Gabriel, Robin Berthier, Etienne Collange, Bertrand Sobesto and Michel Cukier. 2011. Characterizing Attackers and Attacks: An Empirical Study. *17th IEEE Pacific Rim International Symposium on Dependable Computing*.

Schultz, P. Wesley and Jennifer J. Tabanico. 2009. Criminal Beware: A Social Norms Perspective on Posting Public Warning Signs. *Criminology* 47(4):1201-1222.

Schwartz, Richard D. and Sonya Orleans. 1967. On Legal Sanctions. *University of Chicago Law Review* 34(2):274-300.

Shimizu, Katsuhiko. 2007. Prospect Theory, Behavioral Theory, and the Threat-Rigidity Thesis: Combinative Effects on Organizational Decisions to Divest Formerly Acquired Units. *Academy of Management Journal* 50(6):1495-1514.

Simon, Herbert A. 1972. Theories of Bounded Rationality. In *Decision and Organization*, eds. C. B. McGuire and Roy Radner. Minneapolis, MN: University of Minnesota Press.

Slemrod, Joel, Marsha Blumenthal and Charles Christian. 2001. Taxpayer Response to an Increased Probability of Audit: Evidence from a Controlled Experiment in Minnesota. *Journal of Public Economics* 79:455-483.

Spitzner, Lance. 2002. *Honeypots: Tracking Hackers*. Boston, MA: Addison-Wesley Longman.

Spitzner, Lance. 2003. *Honeypots: Definitions and Value of Honeypots*. [accessed online]

Stafford, Mark C. and Mark Warr. 1993. A Reconceptualization of General and Specific Deterrence. *Journal of Research in Crime and Delinquency* 30:123-135.

Taylor, Paul A. 1999. *Hackers*. London, UK: Routledge.

Tittle, Charles R. 1969. Crime Rates and Legal Sanctions. *Social Problems* 16(4):409-423.

Tittle, Charles R. and Alan R. Rowe. 1973. Moral Appeal, Sanction Threat, and Deviance: An Experimental Test. *Social Problems* 20(4):488-498.

Tittle, Charles R. and Alan R. Rowe. 1974. Certainty of Arrest and Crime Rates: A Further Test of the Deterrence Hypothesis. *Social Forces* 52:455-462.

Tombs, Steve and David Whyte. 2013. The Myths and Realities of Deterrence in Workplace Safety Regulation. *British Journal of Criminology* 53:746-763.

VanNostrand, Lisa-Marie and Richard Tewksbury. 1999. The Motives and Mechanics of Operating an Illegal Drug Enterprise. *Deviant Behavior* 20:57-83.

Wang, Wallace. 2003. *Steal This Computer Book 3: What They Won't Tell You About the Internet*. San Francisco, CA: No Starch Press.

Wright, Bradley R. E., Avshalom Caspi, Terrie E. Moffitt and Ray Paternoster. 2004. Does the Perceived Risk of Punishment Deter Criminally Prone Individuals? Rational Choice, Self-Control, and Crime. *Journal of Research in Crime and Delinquency* 41(2):180-212.

Wright, Richard and Scott H. Decker. 1994. *Burglars on the Job: Street Life and Residental Break-Ins.* Boston, MA: Northeastern University Press.

Yano, Yasukata, Michael H. Long and Steven Ross. 1994. The Effects of Simplified and Elaborated Texts on Foreign Language Reading Comprehension. *Language Learning* 44(2):189-219.

Yar, Majid. 2005. Computer Hacking: Just Another Case of Juvenile Delinquency? *The Howard Journal* 44(4):387-399.

Yar, Majid. 2006. *Cybercrime and Society*. London, UK: Sage Publications.

Zimring, Franklin E. and Gordon J. Hawkins. 1973. *Deterrence: The Legal Threat in Crime Control*. Chicago, IL: The University of Chicago Press.